SMD_ST54M_ST_24_002

Security Target for composition

ST54M A01

Document information

This document presents the Common Criteria **Security Target (ST) for composition** of the Security Integrated Circuit **ST54M A01** designed on the **ST54 platform of STMicroelectronics.**

Contents

List of tables

List of figures

1 Introduction (ASE_INT)

1.1 Security Target reference

Table 1. Security Target reference

Document identification	ST54M A01 Security Target for composition
Version number	Rev A01.4, issued in June 2026
Registration	registered at STMicroelectronics under reference SMD_ST54M_ST_24_002

1.2 TOE reference

The Target Of Evaluation (*TOE*[1]) is the **ST54M A01**, a Security Integrated Circuit designed on the **ST54 platform of STMicroelectronics**, with firmware version 4.1.4 .

The reference ST54M A01 completely identifies the *TOE* including its components listed in Table 2 , its guidance documentation detailed in Table 24 .

A01 is the version of the evaluated *TOE*. Any change in the *TOE* components and the guidance documentation leads to a new version of the *TOE*.

The TOE development and production sites are indicated in Table 25 .

Table 2. TOE components

Maskset name	version	Master identification number[2]	Firmware version
K4R0	C	0x02A2	4.1.4

The *IC* maskset name is the product hardware identification.
The *IC* version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the firmware.

Throughout the life of the product, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in Table 2 , and the configuration elements as detailed in the Data Sheet, referenced in Table 24 .

[1] A glossary of terms and abbreviations used in this document is given in Section 10 and Section 11 .
[2] Part of the product information

1.3 Security Target overview

The Target Of Evaluation (TOE referred to in Section 1.2 , is certified under EUCC by the Dutch National Cybersecurity Certification Authority (NCCA) and is developed by the Connected Security division of STMicroelectronics (*ST*).

This multi-assurance Security Target claims conformance to the Eurosmart - Security *IC* Platform Multi-assurance PP-Configurations with Packages [Authentication of the Security *IC*, Cryptographic Services] and PP-Modules [Loader 1 (for usage in secured environment only), Loader 2 (for usage by authorized users only), Address-based Access Control]:

- Security *IC* Platform Protection Profile including Functional Packages ([BSI-CC-PP-0084-V2]) including the functional packages:
  - Package “Authentication of the Security *IC*”
  - Package “Cryptographic Services”
- PP-Modules:
  - “Loader 1 (for usage in secured environment only)”
  - “Loader 2 (for usage by authorized users only)”
  - “Address-based Access Control”

This Security Target defines the following additions to the *PP*:

- Additions for the secure diagnosis capability.

This Security Target defines the following additions to the PP-Module Loader 2 (for usage by authorized users only):

- Additions for the compliance with [Post-Deliv-Load] and specific additions operated in this Security Target.

The SFRs introduced to cover those additions are exclusively drawn from the [CCMB-2022-11-001-R1].

The *TOE* security functionality (*TSF*) consists of the sub-TSFs defined by the PP-Configuration components:
- sub-TSF consisting of the *PP* [BSI-CC-PP-0084-V2] including the selected functional packages and additions for the secure diagnosis,
- sub-TSF Loader 1,
- sub-TSF Loader 2 including the loader 2 additions,
- sub-TSF Address-based Access Control.

The ST54M A01 Security Target claims conformance to a multi-assurance evaluation level:
- A global set of SARs for the *TOE*: EAL5 augmented by ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and ASE_TSS.2.
- A specific set of SARs for each sub-TSF defined in Section 1.8 :
  - For the sub-TSF of the *PP* with additions: the SARs of the global assurance level.
  - For the sub-TSFs Loader 1, Loader 2 and Address-based Access Control: EAL6 augmented with ASE_TSS.2 and ALC_FLR.2.

The intent of this Security Target (*ST*) is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the *TOE*, and to summarize its chosen sub-TSFs services and assurance measures.

Notational conventions:

This *ST* makes various refinements to the above mentioned *PP* and functional packages. They are all properly identified in the text typeset as **indicated here**.

The original text of the [BSI-CC-PP-0084-V2] and [BSI-CC-PP-0125-V1] is repeated as scarcely as possible in this document for reading convenience.

For the sake of clarity, in the following, we will use the notations:

BSI for [BSI-CC-PP-0084-V2] base Protection Profile, BSI.LOADER1 for “Loader 1 (for usage in secured environment only)” PP-module, BSI.LOADER2 for “Loader 2 (for usage by authorized users only)” PP-module including additions denoted by BSI.LOADER2_ADD, BSI.CRYPTO for “Cryptographic Services” functional package, BSI.AUTH for “Authentication of the Security IC” functional package and BSI.MEMORIES for “Address-based Access Control” PP-module and ADD for additions for the secure diagnosis capability.

Organization of the document:

The rest of this Security Target is organized as follows:

- Section 1.4 to Section 1.8 present a description of the *TOE*'s security architecture and features, its life cycle and related environments, the definition of the sub-TSFs.
- Section 2 presents the conformance claims for this Security Target.
- Section 3 to Section 6 define the security problem, the security objectives and the security requirements that apply to the *TOE*.
- Section 7 presents the *TOE* summary specification.
- Section 8 presents the list of *TOE* guidance and *TOE* development sites involved.
- Section 9 presents the list of references.
- A glossary of terms used in this document is given in Section 10 .
- A list of abbreviations used in this document is given in Section 11 .

1.4 TOE overview

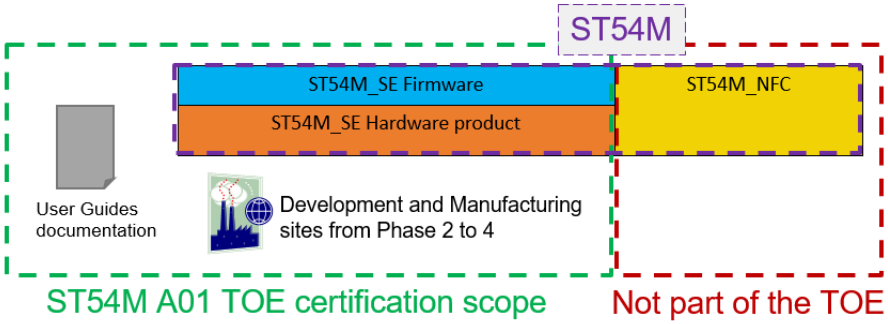
The ST54M A01 is included in the ST54M platform, a near-field communication (*NFC*)-compatible device that comprises a contactless front-end (referred to as the ST54M_CLF), and a secure element (referred to as the ST54M_SE). The ST54M_SE is in the scope of this evaluation, while the **ST54M_CLF is out of scope of this evaluation.**

Furthermore, the ST54M_SE features a MIFARE[3] Classic® cryptographic accelerator called Crypto1, and two specific cryptographic accelerators called SM3 and SM4 which are **all out of the scope of this evaluation.**

In the following, "ST54M A01" and "*TOE*" are used interchangeably.

Figure 1 provides an overview of the ST54M platform.

Figure 1. ST54M platform *TOE* overview



The ST54M A01 is a serial access microcontroller designed for secure mobile applications. It incorporates the most recent generation of Arm® processors for embedded secure systems. Their Arm® Cortex® M35P 32-bit RISC core is built on Armv8-M architecture with additional security features to help to protect against advanced forms of attacks.

The ST54M A01 provides high performance thanks to a fast Cortex® M35P processor, crypto-accelerators and improved Flash memory operation.

The Cortex® M35P core and its cache memory bring great performance and excellent code density thanks to the Thumb®-2 instruction set.

Strong and multiple fault protection mechanisms ensure a guaranteed high-detection coverage that facilitates the development of highly secure software. This is achieved by using two CPUs in locked-step mode, error codes in sensitive memories and hardware logic.

Different derivative devices may be configured depending on the customer needs:

- either by *ST* during the manufacturing or packaging process,
- or by the customer during the packaging, composite product integration, or personalization process.

The derivative devices all share the same hardware design and the same maskset (denoted by the Master identification number). The Master identification number is unique for all product configurations.

[3]MIFARE and MIFARE Classic are trademarks of NXP B.V. and are used under license.

The configuration of the derivative devices is realized in Admin configuration, by *ST* or by the customer. It can impact the availability of the PQC accelerators, MIFARE accelerator, SM3 and SM4 accelerators, as detailed here below:

Table 3. Derivative devices configuration possibilities

Features	Possible values
NVM size	4.5 Mbytes
PQC accelerators	Active, Inactive
MIFARE accelerator (out of scope)	Active, Inactive
SM3 accelerator (out of scope)	Active, Inactive
SM4 accelerator (out of scope)	Active, Inactive

All combinations of different features values are possible and covered by this certification. All possible configurations can vary under a unique *IC*, and without impact on security.

The Master product identification number (MPIN) is unique for all product configurations.
Each derivative device has a specific Child product identification number (PIN), also part of the product information, and specified in ST54M_SE OS developer's guide - User Manual, referenced in Table 24 .

The ST54M A01 embeds firmware that include *IC* Dedicated Software for test and the Loader software as well as the secure boot of the TOE.

The rest of this document applies to all possible configurations of the *TOE*, except when a restriction is mentioned.

In a few words, the ST54M A01 offers a unique combination of high performances and very powerful features for high level security:

- Two instances of the Arm® Cortex® M35P *CPU* connected in Lockstep mode, - Die integrity,
- Monitoring of environmental parameters,
- Highly efficient protection against faults,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- Arm® Cortex® M35P Memory Protection Unit,
- A Library Protection Unit (*LPU*) to isolate protected code,
- Hardware Security Enhanced *DES* accelerator,
- Hardware Security *AES* accelerator,
- NExt Step CRYPTography accelerator (Nescrypt Fast) for public key cryptography algorithms,
- PQC hardware accelerators: Keccak-p, KNTT, DNTT and DMF for post-quantum cryptography algorithms like ML-KEM and ML-DSA.

1.5 TOE description

1.5.1 TOE hardware description

The *TOE* features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks.

The *AES* (Advanced Encryption Standard [fips197] accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in Electronic CodeBook (*ECB*) or Cipher Block Chaining (*CBC*) modes.

The 3-key triple *DES* accelerator (*EDES+*) supports efficiently the Triple Data Encryption Standard (*TDES*) [sp800_67], enabling Electronic Code Book (*ECB*) and Cipher Block Chaining (*CBC*) modes and *DES* computation.

Note that a triple *DES* can be performed by a triple *DES* computation or by 3 single *DES* computations.

The Keccak-p accelerator provides a high-performance implementation for the family of SHA-3 and Keccak hash functions [fips202].

The *NESCRYPT* Fast crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([iso9796], [iso14888], [ieee1363],[ieee1363a], [pkcs1v21], [fips202]. It must be highlighted that Nescrypt provides only primitive operations. It includes several security mechanisms enforcing or supporting several SFRs of the present Security Target, but is not addressing any specific cryptographic *SFR*.

The KNTT, DNTT and DMF accelerators allow fast and secure implementation of the most popular post-quantum cryptosystems such as Kyber for ML-KEM [fips203] and Dilithium for ML-DSA [fips204] with a high level of performance. It must be highlighted that the KNTT, DNTT and DMF accelerators provide only primitive operations. It includes several security mechanisms enforcing or supporting several SFRs of the present Security Target, but is not addressing any specific cryptographic *SFR*.

The *TOE* offers 150 Kbytes of User *RAM* and 4512 Kbytes of secure User high-density Flash memory (*NVM*). An Arm® memory protection unit (*MPU*) enables the user to define its own region organization with specific protection and access permissions. A Library Protection Unit (*LPU*) is available to isolate protected code (e.g. a library) from the rest of the code embedded in the device. LPU's configuration is under the control of ST.

As randomness is a key stone in many applications, the ST54M A01 features a highly reliable True Random Number Generator (*TRNG*), compliant with PTG.2 Class of AIS-31 [bsi_ais_31] .

The *TOE* also provides a 16-bit and 32-bit *CRC* calculation block (compliant to *ISO* 13239, IEEE 802.3, etc.). This CRC is used by the TOE operations and available to users but is not addressing any specific SFR of the present Security Target.

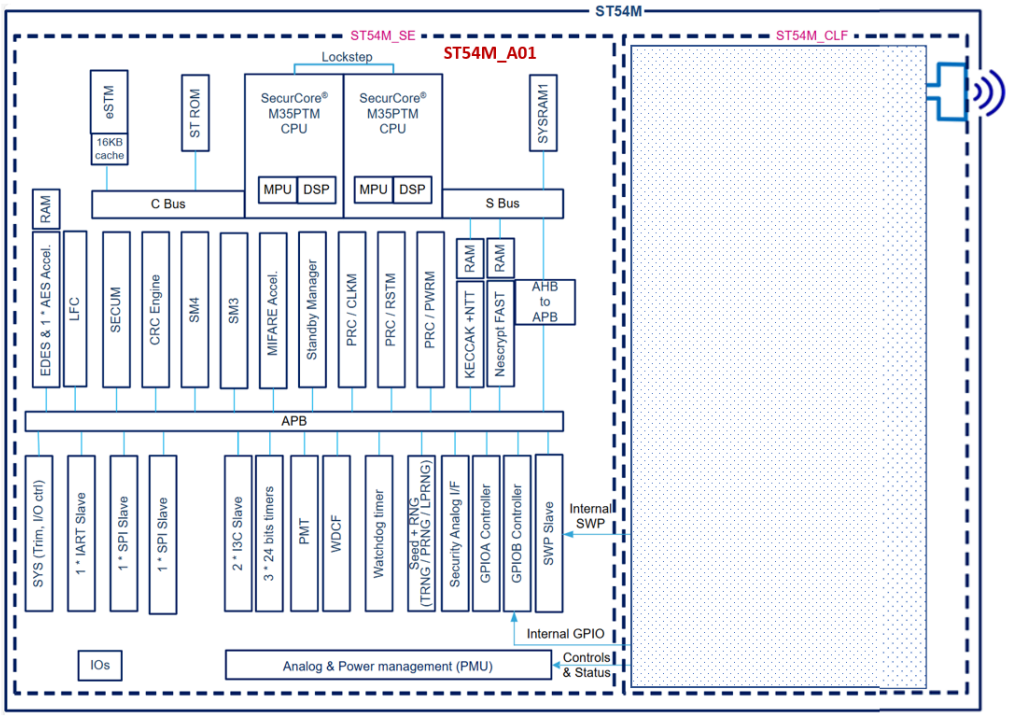
The ST54M platform offers 6 communication interfaces: an *ISO*/IEC 7816-3 slave interface (*IART*), a slave single-wire protocol (*SWP*) interface for communication with a near field communication (*NFC*) router in Secure Element applications, two I3C slave interfaces and two *SPI* slave interfaces for communication in non-SIM applications.

Two general-purpose IO modules (*GPIO*) are available.

The detailed features of this *TOE* are described in the Data Sheet, SE subsystem *OS* developer's guide and in the Cortex® M35P Technical Reference Manual, referenced in Table 24 .

Figure 2 provides the block diagram of the ST54M A01 platform.

Figure 2. ST54M A01 platform block diagram



1.5.2 TOE software description

The *TOE* Firmware includes *IC* Dedicated Software for test (*OST*) in *ROM* and the Loader software as well as the secure boot of the TOE.

The *IC* Dedicated Software provides full test capabilities (operating system for test, called "*OST*"), not accessible by the Security *IC* Embedded Software (*ES*), after *TOE* delivery.

The System *ROM* and *ST NVM* of the *TOE* contain a Dedicated Software (Firmware) which provides:

- a Secure Flash Loader, enabling to securely and efficiently download the Security *IC* Embedded Software (*ES*) into the *NVM*. It also allows the evaluator to load software into the *TOE* for test purpose. The Secure Flash Loader is available in Admin configuration. The customer can choose to activate it in any phase of the product life- cycle under highly secured conditions, or to deactivate it definitely at a certain step.
- low-level functions called Flash Drivers, enabling the Security *IC* Embedded Software (*ES*) to modify and manage the *NVM* contents. The Flash Drivers are available in User configuration.
- a set of protected commands for device testing and product profiling, not intended for the Security *IC* Embedded Software (*ES*) usage, and not available in User configuration.
- a very reduced set of uncritical commands for basic diagnostic purpose (field return analysis), only reserved to STMicroelectronics.
- a set of highly protected commands for secure diagnostic purpose (advanced quality investigations), that can only be operated by STMicroelectronics on its own audited sites. This feature is protected by specific strong access control, completed by environmental measures which prevent access to customer assets.

The Security *IC* Embedded Software (*ES*) is in User *NVM*.

Note: The *ES* is not part of the *TOE* and is out of scope of the evaluation.

1.5.3 *TOE* documentation

The complete list and details of guidance documents is provided in Guidance Documents.

1.5.4 TOE delivery format and method

The ST54M A01 is delivered in package form.

It is shipped to the customer with monitoring of the delivery activity.
The firmware is integrated on the *IC* before delivery.
Guidance documents in pdf format have a reference identifier. Each delivery is registered and done encrypted for each customer by email or using a secure file transfer system.

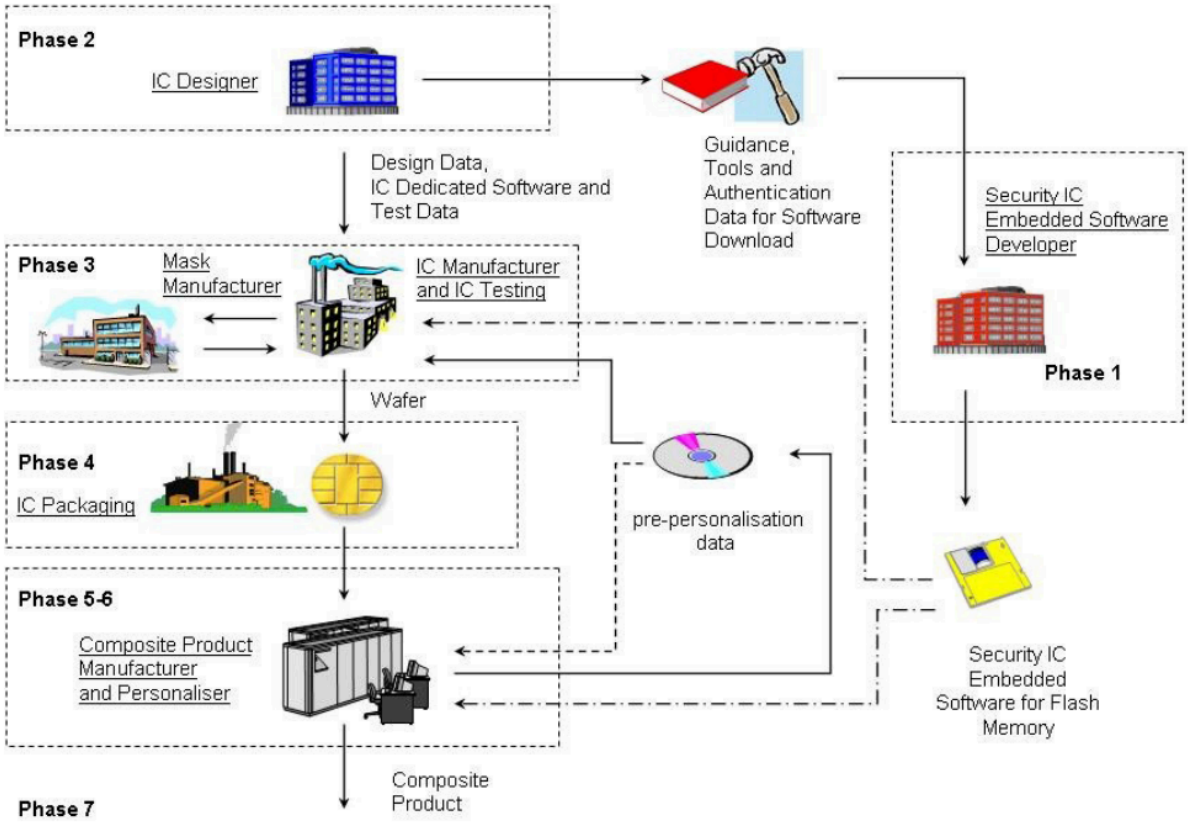
All the possible forms of delivery are equivalent from a security point of view.

1.6 TOE life cycle

This Security Target is fully conform to the claimed *PP*. In the following, just a summary and some useful explanations are given. For complete details on the *TOE* life cycle, please refer to the Eurosmart - Security IC Platform Protection Profile including Functional Packages (BSI-CC-PP-0084-V2), section 1.3.5 [BSI-CC-PP-0084-V2].

The composite product life cycle is decomposed into 7 phases. Each of these phases has the very same boundaries as those defined in the claimed Protection Profile.

Figure 3. **Security IC life cycle**



The life cycle phases are summarized in Table 4 .

The sites potentially involved in the *TOE* life cycle are listed in Table 25 .

The limit of the evaluation corresponds to phases 2, 3 and 4. It also includes the delivery and verification procedures to customer for phase 1, and the TOE delivery either to the *IC* packaging manufacturer or to the composite product integrator. Procedures corresponding to phases 1, 5, 6 and 7 are outside the scope of this evaluation.

In the following, the term “Composite product manufacturing” is uniquely used to indicate phases 1, 5 and 6 all together.
This *ST* also uses the term “Composite product manufacturer” which includes all roles responsible of the *TOE* during phases 1, optionally 4, 5 and 6.

The *TOE* is delivered after Phase 4 packaged form.

In the following, the term “*TOE* delivery” is uniquely used to indicate after Phase 4 (or before Phase 5).

The *TOE* is delivered in Admin (aka Issuer) or User configuration.

Table 4. **Composite product life cycle phases**

Phase	Name	Description
1	Security *IC* embedded software development	security *IC* embedded software development specification of *IC* pre-personalization requirements
2	*IC* development	*IC* design *IC* dedicated software development
3	*IC* manufacturing and testing	integration and photomask fabrication *IC* manufacturing *IC* testing *IC* pre-personalisation

Phase	Name	Description
4	*IC* packaging	security *IC* packaging (and testing) pre-personalisation if necessary
5	Security *IC* product finishing process	composite product finishing process composite product testing
6	Security *IC* personalisation	composite product personalisation composite product testing
7	Security *IC* end usage	composite product usage by its issuers and consumers

1.7 TOE environment

Considering the *TOE*, three types of environments are defined:
- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3 and 4,
- Operational environment, including phase 1 and from phase 5 to phase 7.

1.7.1 *TOE* development environment

To ensure security, the environment in which the development takes place is secured with controllable accesses having traceability. Furthermore, all authorized personnel involved fully understand the importance and the strict implementation of defined security procedures.

The development begins with the *TOE*'s specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

Design and development of the *IC* then follows, together with the dedicated and engineering software and tools development. The engineers use secure computer systems (preventing unauthorized access) to make their developments, simulations, verifications and generation of the *TOE*'s databases. Sensitive documents, files and tools, databases on tapes, and printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

The development centres possibly involved in the development of the *TOE* are denoted by the activity "*DEV*" in Table 25 .

The *IT* support centers potentially involved in the development of the *TOE* are denoted by the activity "*IT*" in Table Table 25 .

1.7.2 *TOE* production environment

Reticules and photomasks are generated from the verified *IC* databases; the former are used in the silicon Wafer-fab processing. As reticules and photomasks are generated off-site, they are transported and worked on in a secure environment. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

The authorized sub-contractors potentially involved in the *TOE* mask manufacturing are denoted by the activity "*MASK*" in Table 25 .

As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all product at all stages of production.

Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and pre-personalization of each *TOE* occurs to assure conformance with the device specification and to load the customer information.

The authorized front-end plant possibly involved in the manufacturing of the *TOE* are denoted by the activity "*FE*" in Table 25 .

The authorized *EWS* plant potentially involved in the testing of the *TOE* are denoted by the activity "*EWS*" in Table 25 .

Wafers are then scribed and broken such as to separate the functional from the non- functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged in phase 4, in a Back_End plant. When testing, programming or deliveries are done offsite, ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

The authorized Back-End plants possibly involved in the packaging of the *TOE* are denoted by the activity "*BE*" in Table 25 .

All sites denoted by the activity "*WHS*" and "*WHSD*" in Table 25 can be involved for the logistics.

1.7.3 *TOE* operational environment

A *TOE* operational environment is the environment of phases 1, then 5 to 7.

At phases 1, 5 and 6, the *TOE* operational environment is a controlled environment.

End-user environments (phase 7): composite products are used in a wide range of applications to assure authorized conditional access.

The ST54M platform products specifically target mobile devices, wearable, smart watch and secure connected devices.

The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid and monitor any abuse of the *TOE*.

1.8 Definition of the sub-TSFs

1.8.1 Sub-TSF of the *PP*

This sub-TSF comprises the core functionality of the Security *IC* Platform as defined in the [BSI-CC-PP-0084-V2], the functional packages "Authentication of the Security IC" and "Cryptographic Services", and the addition for the secure diagnosis capabilities.
The cryptographic services are realized in hardware or hybrid hardware-and-software.

It corresponds to the following SFPs:

- SFP_1: Limited capability and availability Policy / Test
- SFP_2: Data Processing Policy
- SFP_7: Sdiag Limited Capability Policy
- SFP_8: Sdiag Limited Availability Policy

1.8.2 Sub-TSF Address-based Access Control

This sub-TSF corresponds to the PP-Module "Address-based Access Control" of [BSI-CC-PP-0125-V1]. It ensures that access to data, including executable code, is strictly limited based on predefined security attributes associated with memory areas, thus preventing accidental or deliberate memory access violations.

SFP_3: Dynamic Memory Access Control Policy

1.8.3 Sub-TSF Loader 1

This sub-TSF corresponds to the PP-Module Loader of [BSI-CC-PP-0125-V1]. It provides code loading functionality in a controlled environment, strictly limited capabilities and irreversible termination after completion of the loading protect stored user data from unauthorized disclosure and manipulation.

It corresponds to the following SFPs:

- SFP_4: Loader Limited Capability Policy.
- SFP_5: Loader Limited Availability Policy.

1.8.4 Sub-TSF Loader 2

This sub-TSF corresponds to the PP-Module Loader 2 of [BSI-CC-PP-0125-V1]. It provides code loading functionality strictly limited for use by explicitly authorized users. Stringent controls ensure that only authenticated and authorized entities can perform code loading after TOE delivery.

This sub-TSF is extended with the additions for the compliance with [Post-Deliv-Load] including the control of open samples and activation of the loaded code.

It corresponds to the following SFPs:

- SFP_6: Loader SFP.

2 Conformance claims (ASE_CCL)

2.1 Common Criteria conformance claims

The ST54M A01 platform Security Target claims to be conformant to the Common Criteria 2022 revision 1.

More precisely the ST54M A01 platform Security Target is:

- *CC* Part 2 extended, where [CCMB-2022-11-002-R1] is extended with FAU_SAS.1, and,
- *CC* Part 3 conformant, cf. [CCMB-2022-11-003-R1] and,
- *CC* Part 5 conformant, cf. [CCMB-2022-11-005-R1] with,
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), cf. [CCMB-001-ERA].

The extended Security Functional Requirement **FAU_SAS.1** Audit data storage is defined in the Eurosmart - Security *IC* Platform Protection Profile including Functional Packages ([BSI-CC-PP-0084-V2]) and reproduced in Section 5 .

2.2 Package claims

2.2.1 Assurance package claims

The ST54M A01 Security Target claims conformance to a multi-assurance evaluation level:

- A global set of SARs for the *TOE*: EAL5 augmented by ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and ASE_TSS.2.
- A specific set of SARs for each sub-TSF defined in Section 1.8 :
  - For the sub-TSF of the *PP* with additions: the SARs of the global assurance level.
  - For the sub-TSFs Loader 1, Loader 2 and Address-based Access Control: EAL6 augmented with ASE_TSS.2 and ALC_FLR.2.

The refinements of the SARs defined in [BSI-CC-PP-0084-V2] apply.

2.3 PP claims

This multi-assurance Security Target claims strict conformance to the Eurosmart - Security *IC* Platform Multi-assurance PP-Configurations with Packages [Authentication of the Security *IC*, Cryptographic Services] and PP-Modules [Loader 1 (for usage in secured environment only), Loader 2 (for usage by authorized users only), Address-based Access Control].

This Security Target defines the following additions to the *PP*:

- Additions for the secure diagnosis capability.

This Security Target defines the following additions to the PP-Module Loader 2 (for usage by authorized users only):

- Additions for the compliance with [Post-Deliv-Load] and specific additions operated in this Security Target.

The relationship between the PP and the elements included in this Security Target is summarized in Section 2.3.1 and several tables:

- The security environment elements are summarized in Table 9 .
- The security objectives elements are summarized in Table 6 .
- The SFRs are summarized in Table 14 .
- The SARs are summarized in Table 18 .
- A simplified presentation of the TOE Security Policy (*TSP*) is provided along with the SFRs.

2.3.1 PP conformance claims rationale

The *TOE* is a microcontroller designed for secure mobile applications, incorporating hardware and firmware components. The *TOE* implements security mechanisms consistent with the *TOE* type described in [BSI-CC-PP-0125-V1].

The differences between this Security Target security objectives and requirements and those of [BSI-CC-PP-0125-V1], to which conformance is claimed, have been identified and justified in Section 4 and in Section 6 . They have been recalled in the previous section.

In this Security Target, the OSP are those defined in [BSI-CC-PP-0125-V1] while the threats are a superset of those defined in [BSI-CC-PP-0125-V1].

The assumptions in this Security Target are identical to the assumptions in [BSI-CC-PP-0125-V1].

In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the [BSI-CC-PP-0125-V1].

The security problem definition presented in Section 3 , clearly shows the additions to the security problem statement of the PP sub-TSF. These additions are consistent with the SPD defined [BSI-CC-PP-0125-V1] as they concern additional aspects.

The security objectives rationale presented in Section 4.3 clearly identifies modifications and additions made to the rationale presented in the [BSI-CC-PP-0084-V2].

The security objectives are a consistent superset of those defined in PP-Config-Reference. Section 4.3 lists all the security objectives of the Security Target and the additions regarding the [BSI-CC-PP-0125-V1].

Similarly, the security requirements rationale presented in Section 4.3 has been updated with respect to the [BSI-CC-PP-0125-V1].

All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness have been argued in the rationale sections of the present document.

3 Security problem definition (ASE_SPD)

This section describes the security aspects of the environment in which the *TOE* is intended to be used and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions.

Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the [BSI-CC-PP-0125-V1].

A summary of all these security aspects with their respective conditions is provided in Table 5 .

Table 5. Summary of security aspects

	Label	Title
TOE threats	[BSI].T.Leak-Inherent	Inherent Information Leakage
	[BSI].T.Phys-Probing	Physical Probing
	[BSI].T.Malfunction	Malfunction due to Environmental Stress
	[BSI].T.Phys-Manipulation	Physical Manipulation
	[BSI].T.Leak-Forced	Forced Information Leakage
	[BSI].T.Abuse-Func	Abuse of Functionality
	[BSI].T.RND	Deficiency of Random Numbers
	[BSI.AUTH].T.Masquerade_TOE	Masquerade the *TOE*
	[BSI.LOADER1].T.Abuse_Loader1	Abuse the Loader Functionality
	[BSI.LOADER2_ADD].T.Open-Samples-Diffusion	Diffusion of open samples
	[BSI.MEMORIES].T.Addr-Access	Address Access Violation
OSPs	[BSI].P.Process-TOE	Identification during *TOE* Development and Production
	[BSI.LOADER1].P.Lim_Block_Loader1	Limiting and Blocking Loader Functionality
	[BSI.LOADER2].P.Ctrl_Loader2	Controlled usage to Loader Functionality
	[BSI.CRYPTO].P.Crypto-Service	Cryptographic services of the *TOE*
Assumptions	[BSI].A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization
	[BSI].A.Resp-Appl	Treatment of user data of the Composite *TOE*

3.1 Description of assets

Since this Security Target claims strict conformance to the [BSI-CC-PP-0125-V1], the assets defined in the Protection Profile [BSI-CC-PP-0084-V2] are applied and the assets regarding threats are clarified in this Security Target.

The assets (related to the core functionality) to be protected are:
- the user data of the Composite *TOE*,
- the Security *IC* Embedded Software, stored and in operation,
- the security services provided by the *TOE* for the Security *IC* Embedded Software.

The user (consumer) of the *TOE* places value upon the assets related to the following high-level security concerns:

SC1 integrity of user data of the Composite *TOE*,

SC2 confidentiality of user data of the Composite *TOE* being stored in the *TOE*'s protected memory areas,

SC3 correct operation of the security services provided by the *TOE* for the Security *IC* Embedded Software.

Note the Security *IC* Embedded Software is user data and shall be protected while being executed/processed and while being stored in the *TOE*'s protected memories.

The Security *IC* may not distinguish between user data which is public knowledge or confidential. Therefore, the Security *IC* shall protect the user data of the Composite *TOE* in integrity and in confidentiality if stored in protected memory areas, unless the Security *IC* Embedded Software chooses to disclose or modify it.

Integrity of the Security *IC* Embedded Software means that it is correctly being executed which includes the correct operation of the *TOE*'s functionality. Parts of the Security *IC* Embedded Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Security *IC* Embedded Software may need to be kept confidential since specific implementation details may assist an attacker.

This *PP* requires the *TOE* to provide at least one security service: the generation of random numbers by means of a physical Random Number Generator. The section 7 of [BSI-CC-PP-0084-V2] defines optional functional packages for additional security services. The *ST* may address these and/or other security services. It is essential that the *TOE* ensures the correct operation of all the security services provided by the *TOE* for the Security *IC* Embedded Software.

According to this *PP* there is the following high-level security concern related to the random number generation service:

SC4 deficiency of random numbers.

To be able to protect the assets (SC1 to SC4), the *TOE* shall self-protect its *TSF*. Critical information about the *TSF* shall be protected by the development environment and the operational environment. Critical information may include:

- logical design data, physical design data, *IC* Dedicated Software, and Configuration Data,
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photomasks.

Such information and the ability to perform manipulations assist in threatening the above assets.

Note that there are many ways to manipulate or disclose the user data of the Composite *TOE*: An attacker may manipulate the Security *IC* Embedded Software or the *TOE*. An attacker may cause malfunctions of the *TOE* or abuse Test Features provided by the *TOE*. Such attacks usually require design information of the *TOE* to be obtained. They pertain to all information about the circuitry of the *IC* (hardware including the physical memories), the *IC* Dedicated Software with the parts *IC* Dedicated Test Software (if any) and *IC* Dedicated Support Software (if any), and the *TSF* Configuration Data. The knowledge of this information may enable or support attacks on the assets. Therefore, ***ST*** shall ensure that the development and production environment of the *TOE* (refer to 1.3.5) is secure so that no restricted, sensitive, critical or very critical information is unintentionally made available for attacks in the operational phase of the *TOE*.

ST shall apply protection to support the security of the *TOE*. This not only pertains to the *TOE* but also to all information and material exchanged with the developer of the Security *IC* Embedded Software. This covers the Security *IC* Embedded Software itself if provided by the developer of the Security *IC* Embedded Software or any authentication data required to enable the download of software. This includes the delivery (exchange) procedures for Phase 1 and the Phases after *TOE* Delivery as far as they can be controlled by ***ST***. These aspects enforce the usage of the supporting documents and the refinements of *SAR* defined in this *PP*.

The information and material produced and/or processed by ***ST*** in the *TOE* development and production environment (Phases 2 up to *TOE* Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- *IC* Dedicated Software, Initialization Data and Pre-personalization Data,
- Security *IC* Embedded Software, provided by the Security *IC* Embedded Software developer and implemented by the *IC* manufacturer,
- specific development aids,
- test and characterization related data,
- material for software development support, and
- photomasks and products in any form

if they are generated, stored, or processed by ***ST***.

The assets regarding the threats are:

- logical design data, physical design data, *IC* Dedicated Software, and configuration data,
- Initialization data and pre-personalization data, specific development aids, test and characterization related data, material for software development support, and photomasks and product in any form,
- the *TOE* correct operation,
- the Security *IC* Embedded Software, stored in the *TOE*'s protected memories and in operation,
- the security services provided by the *TOE* for the Security *IC* Embedded software,
- the cryptographic co-processors for Triple-DES and *AES*, the random number generator,
- the *TSF* Data.

Application note:
The *TOE* providing a functionality for Security *IC* Embedded Software secure loading into *NVM*, the *ES* is considered as User Data being stored in the *TOE*'s memories at this step, and the Protection Profile corresponding packages are integrated, as well as the requirements from [Post-Deliv-Load].

3.2 Threats

The following threats are described in the [BSI-CC-PP-0084-V2].

Table 6. Threats details

Threats	Description
[BSI].T.Leak-Inherent	Inherent Information Leakage An attacker may exploit information which is leaked from the *TOE* during usage of the Security *IC* in order to disclose confidential user data as part of the assets.
[BSI].T.Phys-Probing	Physical Probing An attacker may perform physical probing of the *TOE* in order to disclose user data while stored in protected memory areas, to disclose/reconstruct the user data while processed or to disclose other critical information about the operation of the *TOE* to enable attacks disclosing or manipulating the user data of the Composite *TOE* or the Security *IC* Embedded Software.
[BSI].T.Malfunction	Malfunction due to Environmental Stress An attacker may cause a malfunction of *TSF* or of the Security *IC* Embedded Software by applying environmental stress in order to modify security services of the *TOE* or modify functions of the Security *IC* Embedded Software deactivate or affect security mechanisms of the *TOE* to enable attacks.
[BSI].T.Phys-Manipulation	Physical Manipulation An attacker may physically modify the Security *IC* in order to modify user data of the Composite *TOE*, modify the Security *IC* Embedded Software, modify or deactivate security services of the *TOE*, or modify security mechanisms of the *TOE* to enable attacks disclosing or manipulating the user data of the Composite *TOE* or the Security *IC* Embedded Software.
[BSI].T.Leak-Forced	Forced Information Leakage An attacker may exploit information which is leaked from the *TOE* during usage of the Security *IC* in order to disclose confidential user data of the Composite *TOE* as part of the assets even if the information leakage is not inherent but caused by the attacker.
[BSI].T.Abuse-Func	Abuse of Functionality An attacker may use functions of the *TOE* which may not be used after *TOE* Delivery in order to disclose or manipulate user data of the Composite *TOE*, manipulate (explore, bypass, deactivate or change) security services of the *TOE* or manipulate (explore, bypass, deactivate or change) functions of the Security *IC* Embedded Software or enable an attack disclosing or manipulating the user data of the Composite *TOE* or the Security *IC* Embedded Software.
[BSI].T.RND	Deficiency of Random Numbers

Threats	Description
	An attacker may predict or obtain information about random numbers generated by the *TOE* security service for instance because of a lack of entropy of the random numbers provided.
[BSI.AUTH].T.Masquerade_TOE	Masquerade the *TOE* An attacker may threaten the property being a genuine *TOE* by producing a chip which is not a genuine *TOE* but wrongly identifying itself as genuine *TOE* sample.
[BSI.LOADER1].T.Abuse_Loader1	Abuse the Loader Functionality An attacker may use the Loader functionality after *TOE* Delivery to disclose or manipulate stored user data.
[BSI.LOADER2_ADD].T.Open-Samples-Diffusion	Diffusion of open samples An attacker may get access to open samples of the *TOE* and use them to gain information about the *TSF* (loader, memory management unit, *ROM* code, …). He may also use the open samples to characterize the behavior of the *IC* and its security functionalities (for example: characterization of side channel profiles, perturbation cartography, …). The execution of a dedicated security features (for example: execution of a *DES* computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the *IC*.
[BSI.MEMORIES].T.Addr-Access	Address Access Violation An agent, e.g. a part of the Security *IC* Embedded Software, accidentally or deliberately, accesses a memory, memory mapped peripheral or any addressable object without authorization, leading to a compromise (disclosure or modification) of the code or data stored at that address, or to operation disruption. Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access. Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

3.3 Organizational security policies

ST applies the Protection policy during *TOE* Development and Production ([BSI].P.ProcessTOE) as specified below.

[BSI.LOADER1].P.Lim-Block-Loader1 and [BSI.LOADER2].P.Ctrl-Loader2 are dedicated to the Secure Flash Loader, and described in the [BSI-CC-PP-0084-V2] packages “Loader 1 (for usage in secured environment only)” and “Loader 2 (for usage by authorized users only)”. [BSI.LOADER2].P.Ctrl-Loader2 has been completed in accordance with [Post-Deliv-Load] and additions to the Loader2.

[BSI.CRYPTO].P.Crypto-Service provides secure hardware-based cryptographic services for the Security *IC* Embedded Software, it is described in [BSI-CC-PP-0084-V2] Cryptographic Services package.

The following security policies are described in the [BSI-CC-PP-0084-V2].

Table 7. OSPs details

OSPs	Description
[BSI].P.Process-TOE	Identification during *TOE* Development and Production

OSPs	Description
	An accurate identification is established for the *TOE*. This requires that each instantiation of the *TOE* carries this unique identification.
[BSI.LOADER1].P.Lim_Block_Loader1	Limiting and Blocking Loader Functionality The Composite Product Manufacturer uses the Loader for loading user data, and also *IC* Dedicated Support Software in charge of the *IC* Manufacturer. He limits the capability and blocks the availability of the Loader[4] in order to protect stored user data from disclosure and manipulation.
[BSI.LOADER2].P.Ctrl_Loader2	Controlled usage to Loader Functionality The authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation. The activation of the loaded Additional ~~Code~~ **user data** is possible if: • integrity and authenticity of the Additional ~~Code~~ **user data** have been successfully checked; • the loaded ~~Additional Code~~ **user data** is targeted to the Initial *TOE* (Identification ~~Data~~ of the Additional ~~Code~~ **user data** and the Initial *TOE* will be used for this check). Identification ~~Data~~ of the resulting Final *TOE* shall identify the Initial *TOE* and the ~~activated~~ Additional ~~Code~~ **user data**. Identification Data shall be protected in integrity. Note: Here, the term *TOE* denotes the *TOE* itself as well as the composite *TOE* which both may be maintained by loading of data.
[BSI.CRYPTO].P.Crypto-Service	Cryptographic services of the *TOE* The *TOE* provides secure hardware-based cryptographic services for the Security *IC* Embedded Software. The *TOE* shall provide the following specific security functionality to the Security *IC* Embedded Software: • Triple Data Encryption Standard (*TDES*), • Advanced Encryption Standard (*AES*). • Keccak hash functions (Keccak-p)

3.4 Assumptions

The following assumptions are described in the [BSI-CC-PP-0084-V2] section 3.4.

Table 8. Assumptions details

Assumptions	Description
[BSI].A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization It is assumed that security procedures are used after delivery of the *TOE* by the *TOE* Manufacturer up to delivery to the End-consumer to maintain confidentiality and integrity of the *TOE* and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
[BSI].A.Resp-Appl	Treatment of user data of the Composite *TOE* All user data of the Composite *TOE* are under the control of the Security *IC* Embedded Software. Therefore, it is assumed that security relevant user data of the Composite *TOE* (especially cryptographic keys) are treated by the Security *IC* Embedded Software as defined for its specific application context.

[4] Note that blocking the loader is not required, as only authorized users can use the Loader as stated in [BSI.LOADER2].P.Ctrl_Loader2

3.5 SPD of the sub-TSFs

3.5.1 Sub-TSF PP-0084-v2

The security problem definition for the PP-0084-v2 sub-TSF corresponds to the subset of the global SPD defined earlier in Section 3 , consisting of:

- all assets, threats, organizational security policies, and assumptions defined in Table 5 except those specifically defined in Section Section 3.5.2 , Section Section 3.5.3 and Section Section 3.5.4 .
- the SPD introduced by the Authentication of the Security *IC* package and
- the SPD introduced by the Cryptographic Services package.

No new assets, threats, OSPs or assumptions are introduced beyond those already defined in the global SPD.

3.5.2 Sub-TSF Loader 1

The SPD of this sub-TSF is defined in the PP-Module “Loader 1 (for usage in secured environment only)” from [BSI-CC-PP-0125-V1]:

- [BSI.LOADER1].T.Abuse_Loader1 “Abuse the Loader Functionality”
- [BSI.LOADER1].P.Lim_Block_Loader1 “Limiting and Blocking Loader Functionality”

3.5.3 Sub-TSF Loader 2

The SPD of this sub-TSF is defined in the PP-Module “Loader 2 (for usage by authorized users only)” from [BSI-CC-PP-0125-V1]:

- [BSI.LOADER2].P.Ctrl_Loader2 “Controlled usage to Loader Functionality”

The following objective is an additional one based on [Post-Deliv-Load] and security target operated.

- [BSI.LOADER2_ADD].T.Open-Samples-Diffusion “Diffusion of open samples”

3.5.4 Sub-TSF Address-based Access Control

The SPD of this sub-TSF is defined in the PP-Module “Address-based Access Control” from [BSI-CC-PP-0125-V1]:

- [BSI.MEMORIES].T.Addr-Access “Address Access Violation”

4 Security objectives (ASE_OBJ)

The security objectives of the *TOE* cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the *TOE* and associated documentation during development and production phases,
- provide random numbers,
- provide cryptographic support,
- provide access control functionality.

Note that the origin of each security objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the [BSI-CC-PP-0125-V1].

A summary of all the *TOE* security objectives is provided in Table 9 .

Table 9. Summary of security objectives

	Label	Title
TOE	[BSI].O.Leak-Inherent	Protection against Inherent Information Leakage
	[BSI].O.Phys-Probing	Protection against Physical Probing
	[BSI].O.Malfunction	Protection against Malfunctions
	[BSI].O.Phys-Manipulation	Protection against Physical Manipulation
	[BSI].O.Leak-Forced	Protection against Forced Information Leakage
	[BSI].O.Abuse-Func	Protection against Abuse of Functionality
	[BSI].O.Identification	*TOE* Identification
	[BSI].O.RND	Random Numbers
	[BSI.AUTH].O.Authentication	Authentication to external entities
	[BSI.LOADER1].O.Cap_Avail_Loader1	Capability and availability of the Loader
	[BSI.LOADER2].O.Ctrl_Auth_Loader2	Access control and authenticity for the Loader
	[BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality	Protection of the confidentiality of the *TSF*
	[BSI.LOADER2_ADD].O.Secure-UC-Code	Secure loading of the Update Code
	[BSI.LOADER2_ADD].O.Secure-UC-Activation	Secure activation of the Update Code
	[BSI.LOADER2_ADD].O.TOE-Identification	Secure identification of the *TOE*
	[BSI.LOADER2_ADD].O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image
	[BSI.LOADER2_ADD].O.MemImage-Identification	Secure identification of the Memory Image
	[BSI.CRYPTO].O.Crypto-Service	Cryptographic services
	[BSI.MEMORIES].O.Addr-Access	Address-based Access Control
Environments	[BSI].OE.Resp-Appl	Treatment of user data of the Composite *TOE*
	[BSI].OE.Process-Sec-IC	Protection during composite product manufacturing
	[BSI.AUTH].OE.TOE_Auth	External entities authenticating of the *TOE*
	[BSI.LOADER1].OE.Lim_Block_Loader1	Limitation of capability and blocking the Loader
	[BSI.LOADER2].OE.Usage_Loader2	Secure communication and usage of the Loader
	[BSI.LOADER2_ADD].OE.Composite-TOE-Id	Composite *TOE* identification
	[BSI.LOADER2_ADD].OE.TOE-Id	*TOE* identification
	[ADD].OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic

4.1 Security objective for the TOE

The following security objectives are described in the [BSI-CC-PP-0084-V2].

Table 10. Security objectives details

Security objectives	Description
[BSI].O.Leak-Inherent	Protection against Inherent Information Leakage The *TOE* shall provide protection against disclosure of confidential data stored and/or processed in the Security *IC*: • by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or *I/O* lines) and • by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or *I/O* lines).
[BSI].O.Phys-Probing	Protection against Physical Probing The *TOE* shall provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the *TOE*. This includes protection against • measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or • measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and *IC* failure analysis) with a prior reverse-engineering to understand the design and its properties and functions. The *TOE* shall be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.
[BSI].O.Malfunction	Protection against Malfunctions The *TOE* shall ensure its correct operation. The *TOE* shall indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.
[BSI].O.Phys-Manipulation	Protection against Physical Manipulation The *TOE* shall provide protection against manipulation of the *TOE* (including its software and *TSF* data), the Security *IC* Embedded Software and the user data of the Composite *TOE*. This includes protection against • reverse-engineering (understanding the design and its properties and functions), • manipulation of the hardware and any data, as well as • undetected manipulation of memory contents.
[BSI].O.Leak-Forced	Protection against Forced Information Leakage The *TOE* shall be protected against disclosure of confidential data processed in the Security *IC* (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker. • by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or

Security objectives	Description
	• by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”. If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.
[BSI].O.Abuse-Func	Protection against Abuse of Functionality The *TOE* shall prevent that functions of the *TOE* which may not be used after *TOE* Delivery can be abused in order to disclose critical user data of the Composite *TOE*, manipulate critical user data of the Composite *TOE*, manipulate Security *IC* Embedded Software or bypass, deactivate, change or explore security features or security services of the *TOE*.
[BSI].O.Identification	*TOE* Identification The *TOE* shall provide means to store Initialization Data and Pre-personalization Data in its non-volatile memory. The Initialization Data (or parts of them) are used for *TOE* identification.
[BSI].O.RND	Random Numbers The *TOE* shall ensure the cryptographic quality of random number generation. For instance, random numbers shall not be predictable and shall have a sufficient entropy. The *TOE* shall ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.
[BSI.AUTH].O.Authentication	Authentication to external entities The *TOE* shall be able to authenticate itself to external entities. The Initialization Data (or parts of them) are used as *TOE* authentication reference data.
[BSI.LOADER1].O.Cap_Avail_Loader1	Capability and availability of the Loader The *TOE* shall provide limited Loader capabilities and irreversible termination of the Loader in order to protect stored user data from disclosure and manipulation.
[BSI.LOADER2].O.Ctrl_Auth_Loader2	Access control and authenticity for the Loader The *TOE* shall provide a trusted communication channel with the authorized user, support the confidentiality protection and the authentication of the user data to be loaded, and control the access to the Loader functionality.
[BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality	Protection of the confidentiality of the *TSF* The *TOE* must provide protection against disclosure of confidential operations of the Security *IC* (loader, memory management unit, …) through the use of a dedicated code loaded on open samples.
[BSI.LOADER2_ADD].O.Secure-UC-Code	Secure loading of the Update Code The Loader of the ~~Initial~~ *TOE* shall check an evidence of authenticity and integrity of the loaded Update Code. The Loader enforces that only the allowed version of the Update Code can be loaded on the Initial *TOE*. The Loader shall forbid the loading of an Update Code not intended to be assembled with the Initial *TOE*. During the Load Phase of an Update Code, the *TOE* shall remain secure. Note: Concretely, the *TOE* manages the Update Code as an Additional Memory Image.
[BSI.LOADER2_ADD].O.Secure-UC-Activation	Secure activation of the Update Code Activation of the Update Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Updated *TOE* shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Updated *TOE*, otherwise (in case of interruption or incident which prevents the forming of the Updated *TOE*), the Initial *TOE* shall remain in its initial state or fail secure.
[BSI.LOADER2_ADD].O.TOE-Identification	Secure identification of the *TOE*

Security objectives	Description
	The Identification Data identifies the Initial *TOE* and Update Code. The *TOE* provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Update Code, the Identification Data of the Final *TOE* allows identifications of Initial *TOE* and Update code. The user shall be able to uniquely identify Initial *TOE* and Update Code(s) which are embedded in the Final *TOE*.
[BSI.LOADER2_ADD].O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image The Loader of the *TOE* shall check an evidence of authenticity and integrity of the loaded Memory Image. The Loader enforces that only the allowed version of the Additional Memory Image can be loaded after the Initial Memory Image. The Loader shall forbid the loading of an Additional Memory Image not intended to be assembled with the Initial Memory Image. Note: This objective is similar to [BSI.LOADER2_ADD].O.Secure-UC-Code, applied to user data (e.g. embedded software).
[BSI.LOADER2_ADD].O.MemImage-Identification	Secure identification of the Memory Image The Identification Data identifies the Initial Memory Image and Additional Memory Image. The *TOE* provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. Storage of the Additional Memory Image and update of the Identification Data shall be performed at the same time in an Atomic way, otherwise (in case of interruption or incident which prevents this alignment), the Memory Image shall remain in its initial state or the *TOE* shall fail secure. The Identification Data of the Final Memory Image allows identifications of Initial Memory Image and Additional Memory Image. Note: This objective is similar to [BSI.LOADER2_ADD].O.Secure-UC-Activation and [BSI.LOADER2_ADD].O.TOE-Identification, applied to user data (e.g. embedded software).
[BSI.CRYPTO].O.Crypto-Service	Cryptographic services The *TOE* shall provide secure hardware-based cryptographic services implementing cryptographic algorithms. The *TOE* shall provide the following specific security functionality to the Security *IC* Embedded Software: • Triple Data Encryption Standard (*TDES*), • Advanced Encryption Standard (*AES*). • Keccak hash functions (Keccak-p)
[BSI.MEMORIES].O.Addr-Access	Address-based Access Control The *TOE* shall allow the Security *IC* Embedded Software to define restricted address-based areas and shall enforce their partitioning so that only authorized operations can be performed by authorized entities within restricted areas.

4.2 Security objectives for the environment

Clarification related to “Treatment of User Data of the Composite *TOE* ([BSI].OE.Resp-Appl)”: by definition cipher or plain text data and cryptographic keys are User Data. The Security *IC* Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the *TOE* and use keys and functions appropriately in order to ensure the strength of cryptographic operation. This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the *TOE* and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

Security Objectives for the Security *IC* Embedded Software development environment (phase 1):

Table 11. Operational Environment details

Operational Environment	Description	Phase
[BSI].OE.Resp-Appl	Treatment of user data of the Composite *TOE* Security relevant user data of the Composite *TOE* (especially cryptographic keys) shall be treated by the Security *IC* Embedded Software as required by the security needs of the specific application context.	Up to phase 1

Security Objectives for the operational Environment (phase 4 up to 7):

Table 12. Operational Environment details

Operational Environment	Description	Phase
[BSI].OE.Process-Sec-IC	Protection during composite product manufacturing Security procedures shall be used after *TOE* Delivery up to delivery to the End-consumer to maintain confidentiality and integrity of the *TOE* and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).	Up to phase 6
[BSI.AUTH].OE.TOE_Auth	External entities authenticating of the *TOE* The operational environment shall support the authentication verification mechanism and know the authentication reference data of the *TOE*.	Up to phase 7
[BSI.LOADER1]. OE.Lim_Block_Loader1	Limitation of capability and blocking the Loader The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and, **if desired**, terminate irreversibly the Loader after intended usage of the Loader. *Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl_Loader2.*	Up to phase 6
[BSI.LOADER2]. OE.Usage_Loader2	Secure communication and usage of the Loader The authorized user shall support the trusted communication channel with the *TOE* by enforcing the confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader. *The authorized user must organize the maintenance transactions to ensure that the additional code (loaded as data) is able to operate as in the Final composite* TOE. *The authorized user must manage and associate unique Identification to the loaded data.*	Up to phase 7
[BSI.LOADER2_ADD]. OE.Composite-TOE-Id	Composite *TOE* identification The composite manufacturer must maintain a unique identification of a composite *TOE* under maintenance.	Up to phase 7
[BSI.LOADER2_ADD]. OE.TOE-Id	*TOE* identification The *IC* manufacturer must maintain a unique identification of the *TOE* under maintenance.	Up to phase 7
[ADD].OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic The *IC* manufacturer must support the trusted communication channel with the *TOE* by fulfilling the access conditions required by the secure Diagnostic. The *IC* manufacturer must manage the Secure Diagnostic transactions so that they cannot be used to disclose critical user data of the Composite *TOE*, manipulate critical user data of the Composite *TOE*, manipulate Security *IC* Embedded Software or bypass, deactivate, change or explore security features or security services of the *TOE*.	Up to phase 7

4.3 Security objectives rationale

The main line of this rationale is that the inclusion of all the security objectives of the [BSI-CC-PP-0125-V1], together with those introduced in this *ST*, guarantees that all the security environment aspects identified in Section 3 are addressed by the security objectives stated in this chapter.

Thus, it is necessary to show that:

- security environment aspects from this *ST*, are addressed by security objectives stated in this chapter,
- security objectives from this *ST*, are suitable (i.e. they address security environment aspects),
- security objectives from this *ST*, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).

The augmentation made in this ST introduces the following security environment aspect:

- TOE threats “Diffusion of open samples [BSI.LOADER2_ADD].T.Open-Samples-Diffusion”.

The justification of the additional policies, additional threats, and additional assumptions provided in the next subsections shows that they do not contradict to the rationale already given in the Protection Profile [BSI-CC-PP-0084-V2] for the assumptions, policy and threats defined there.

Table 13. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organizational Security Policy	Security Objectives	Notes
[BSI].T.Leak-Inherent	[BSI].O.Leak-Inherent	
[BSI].T.Phys-Probing	[BSI].O.Phys-Probing	
[BSI].T.Malfunction	[BSI].O.Malfunction	
[BSI].T.Phys-Manipulation	[BSI].O.Phys-Manipulation	
[BSI].T.Leak-Forced	[BSI].O.Leak-Forced	
[BSI].T.Abuse-Func	[BSI].O.Abuse-Func [ADD].OE.Secure-Diag-Usage	
[BSI].T.RND	[BSI].O.RND	
[BSI.AUTH].T.Masquerade_TOE	[BSI.AUTH].O.Authentication [BSI.AUTH].OE.TOE_Auth	
[BSI.LOADER1].T.Abuse_Loader1	[BSI.LOADER1].O.Cap_Avail_Loader1 [BSI.LOADER1].OE.Lim_Block_Loader1	
[BSI.LOADER2_ADD].T.Open-Samples-Diffusion	[BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality [BSI].O.Leak-Inherent [BSI].O.Leak-Forced	
[BSI.MEMORIES].T.Addr-Access	[BSI.MEMORIES].O.Addr-Access	
[BSI].P.Process-TOE	[BSI].O.Identification	Phases 2-3 optional Phase 4
[BSI.LOADER1].P.Lim_Block_Loader1	[BSI.LOADER1].O.Cap_Avail_Loader1 [BSI.LOADER1].OE.Lim_Block_Loader1	
[BSI.LOADER2].P.Ctrl_Loader2	[BSI.LOADER2].O.Ctrl_Auth_Loader2 [BSI.LOADER2].OE.Usage_Loader2 [LOADER2_ADD].O.Secure-UC-Activation [LOADER2_ADD].O.Secure-UC-Code [LOADER2_ADD].O.TOE-Identification [LOADER2_ADD].O.Secure-Load-AMemImage [LOADER2_ADD].O.MemImage-Identification [LOADER2_ADD].OE.TOE-Id [LOADER2_ADD].OE.Composite-TOE-Id	
[BSI.CRYPTO].P.Crypto-Service	[BSI.CRYPTO].O.Crypto-Service	

Assumption, Threat or Organizational Security Policy	Security Objectives	Notes
[BSI].A.Process-Sec-IC	[BSI].OE.Process-Sec-IC	Phases 5-6 optional Phase 4
[BSI].A.Resp-Appl	[BSI].OE.Resp-Appl	Phase 1

4.3.1 TOE threat Inherent Information Leakage

The justification related to the threat “Inherent Information Leakage, ([BSI].T.Leak-Inherent)” is as follows:

It is clear from the description of [BSI].O.Leak-Inherent, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.2 TOE threat Physical Probing

The justification related to the threat “Physical Probing, ([BSI].T.Phys-Probing)” is as follows:

It is clear from the description of [BSI].O.Phys-Probing, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.3 TOE threat Malfunction due to Environmental Stress

The justification related to the threat “Malfunction due to Environmental Stress, ([BSI].T.Malfunction)” is as follows:

It is clear from the description of [BSI].O.Malfunction, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.4 TOE threat Physical Manipulation

The justification related to the threat “Physical Manipulation, ([BSI].T.Phys-Manipulation)” is as follows:

It is clear from the description of [BSI].O.Phys-Manipulation, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.5 TOE threat Forced Information Leakage

The justification related to the threat “Forced Information Leakage, ([BSI].T.Leak-Forced)” is as follows:

It is clear from the description of [BSI].O.Leak-Forced, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.6 TOE threat Abuse of Functionality

The justification related to the threat “Abuse of Functionality, ([BSI].T.Abuse-Func)” is as follows:

It is clear from the description of [BSI].O.Abuse-Func, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds. The objective [BSI].O.Abuse-Func is supported by the security objectives for the operational environment [ADD].OE.Secure-Diag-Usage for the particular case of the Secure Diagnostic.
Therefore [BSI].T.Abuse-Func is covered by these three objectives.

4.3.7 TOE threat Deficiency of Random Numbers

The justification related to the threat “Deficiency of Random Numbers, ([BSI].T.RND)” is as follows:

It is clear from the description of [BSI].O.RND, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

4.3.8 TOE threat Masquerade the *TOE*

The justification related to the threat “Masquerade the *TOE*, ([BSI.AUTH].T.Masquerade_TOE)” is as follows:

The threat “Masquerade the *TOE*, ([BSI.AUT].T.Masquerade_TOE)” is directly covered by the *TOE* security objective “Authentication to external entities ([BSI.AUT].O.Authentication)” describing the proving part of the authentication and the security objective for the operational environment of the *TOE* “External entities authenticating of the *TOE* ([BSI.AUT].OE.TOE_Auth)” the verifying part of the authentication.

4.3.9 TOE threat Abuse the Loader Functionality

The justification related to the threat “Abuse the Loader Functionality, ([BSI.LOADER1].T.Abuse_Loader1)” is as follows:

The *TOE* security objective “Capability and availability of the Loader” ([BSI.LOADER1].O.Cap_Avail_Loader1)” mitigates also the threat “Abuse of Loader Functionality “ ([BSI.LOADER1].T.Abuse_Loader1) if attacker tries to misuse the Loader functionality in order to manipulate security services of the *TOE* provided or depending on *IC* Dedicated Support Software or user data of the *TOE* as Security *IC* Embedded Software, *TSF* data or user data of the Composite Product.
The organizational security policy “Limitation and Blocking the Loader Functionality ([BSI.LOADER1].OE.Lim_Block_Loader1)” is directly implemented by the security objective for the *TOE* “Capability and availability of the Loader ([BSI.LOADER1].O.Cap_Avail_Loader1)” and contributes to cover the threat (BSI.LOADER1.T.Abuse_Loader1).

4.3.10 TOE threat Diffusion of open samples

The justification related to the threat “Diffusion of open samples, ([BSI.LOADER2_ADD].T.Open-Samples-Diffusion)” is as follows:

According to threat [BSI.LOADER2_ADD].T.Open-Samples-Diffusion, the TOE shall provide protection against attacks using open samples of the TOE to characterize the behavior of the IC and its security functionalities. The objective [BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality requires protection against disclosure of confidential operations of the Security IC through the use of a dedicated code loaded on open samples. Additionally, [BSI].O.Leak-Inherent and [BSI].O.Leak-Forced ensures protection against disclosure of confidential data processed in the Security IC. Therefore [BSI.LOADER2_ADD].T.Open-Samples-Diffusion is covered by these three objectives.

The added objective for the TOE [BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality does not introduce any contradiction in the security objectives for the TOE.

4.3.11 TOE threat Address Access Violation

The justification related to the threat “Address Access Violation, ([BSI.MEMORIES].T.Addr-Access)” is as follows:

According to [BSI.AAC].O.Addr-Access the *TOE* shall enforce the definition and partitioning of restricted address-based areas, as specified by the Security *IC* Embedded Software. The *TOE* ensures that only authorized operations are executed by authorized entities within these restricted areas. By enforcing this partitioning, the *TOE* prevents security violations resulting from unauthorized or accidental access to protected address regions, which may include sensitive data or code.
The threat ([BSI.AAC].T.Addr-Access) is therefore mitigated if this objective is met.

The added objective for the *TOE* [BSI.AAC].O.Addr-Access does not introduce any contradiction in the security objectives for the *TOE*.

4.3.12 Organizational security policy Identification during *TOE* Development and Production

The justification related to the organizational security policy “Identification during *TOE* Development and Production, ([BSI].P.Process-TOE)” is as follows:

[BSI].O.Identification requires that the TOE supports the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment, the production environment shall support the integrity of the generated unique identification.
The technical and organizational security controls that ensure the security of the development environment and production environment are evaluated based on the assurance controls that are part of the evaluation. All listed items and the associated development and production environments are subject of the evaluation. Therefore, the organizational security policy [BSI].P.Process-TOE is covered by this objective, as far as organizational controls are concerned.

4.3.13 Organizational security policy Limiting and Blocking Loader Functionality

The justification related to the organizational security policy “Limiting and Blocking Loader Functionality, ([BSI.LOADER1].P.Lim_Block_Loader1)” is as follows:

The organizational security policy “Limitation and Blocking the Loader Functionality ([BSI.LOADER1].OE.Lim_Block_Loader1)” is directly implemented by the security objective for the *TOE* “Capability and availability of the Loader ([BSI.LOADER1].O.Cap_Avail_Loader1)”.

4.3.14 Organizational security policy Controlled usage to Loader Functionality

The justification related to the organizational security policy “Controlled usage to Loader Functionality, ([BSI.LOADER2].P.Ctrl_Loader2)” is as follows:

As stated in [BSI-CC-PP-0084-V2], the organizational security policy “Controlled usage to Loader Functionality ([BSI.LOADER2].P.Ctrl_Loader2) is implemented by the security objective for the *TOE* “Access control and authenticity for the Loader ([BSI.LOADER2].O.Ctrl_Auth_Loader2)“ and the security objective for the *TOE* environment “Secure communication and usage of the Loader ([BSI.LOADER2].OE.Loader_Usage2)”.
The security objectives “Secure loading of the Additional Code ([LOADER2_ADD].O.Secure-UC-Code)”, “Secure activation of the Additional Code ([LOADER2_ADD].O.Secure-UC-Activation)”, and ”Secure identification of the *TOE* ([LOADER2_ADD].O.TOE-Identification)” specified by [Post-Deliv-Load] additionally enforce this policy since they require authenticity, atomicity, identification of the loaded additional code, part of the *TOE*. ”Secure identification of the *TOE* ([LOADER2_ADD].O.TOE-Identification)” is supported by the security objective for the *TOE* environment “*TOE* identification ([ADD].O.TOE-Id)”.
Similarly, the security objectives “Secure loading of the Additional Memory Image ([LOADER2_ADD].O.Secure-Load-AMemImage)”, and “Secure identification of the Memory Image ([LOADER2_ADD].O.MemImage-Identification)”, enforce this policy since they require authenticity, atomicity, identification of the loaded additional memory image for the user data (embedded software). ”Secure identification of Memory Image ([LOADER2_ADD].O.Secure-Load-AMemImage)” is supported by the security objective for the *TOE* environment “Composite *TOE* identification ([BSI.LOADER2_ADD].OE.Composite-TOE-Id)”.
Therefore the policy “Controlled usage to Loader Functionality, ([BSI.LOADER2].P.Ctrl_Loader2)” is covered by these nine objectives.

4.3.15 Organizational security policy Cryptographic services of the *TOE*

The justification related to the organizational security policy “Cryptographic services of the *TOE*, ([BSI.CRYPTO].P.Crypto-Service)” is as follows:

The organizational security policy ‘Cryptographic services of the *TOE*’ ([BSI.CRYPTO].P.Crypto-Service) is implemented directly by the *TOE* security objective ‘Cryptographic Algorithm’ ([BSI.CRYPTO].O.Crypto-Service).

Nevertheless the security objectives [BSI].O.Leak-Inherent, [BSI].O.Phys-Probing, [BSI].O.Malfunction, [BSI].Phys-Manipulation and [BSI].Leak-Forced define how to implement the specific security functionality required by [BSI.CRYPTO].P.Crypto-Service. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from [BSI.CRYPTO].P.Crypto-Service.) Especially BSI.O.Leak-Inherent and [BSI].O.Leak-Inherent refer to the protection of confidential data (User Data or *TSF* data) in general. User Data are also processed by the specific security functionality required by [BSI.CRYPTO].P.Crypto-Service.

4.3.16 Assumption Protection during Packaging, Finishing and Personalization

The justification related to the assumption “Protection during Packaging, Finishing and Personalization, ([BSI].A.Process-Sec-IC)” is as follows:

Since [BSI].OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in [BSI].A.Process-Sec-IC, the assumption is covered by this objective.

4.3.17 Assumption Treatment of user data of the Composite *TOE*

The justification related to the assumption “Treatment of user data of the Composite *TOE*, ([BSI].A.Resp-Appl)” is as follows:

Since [BSI].OE.Resp-Appl requires the Security *IC* Embedded Software to implement measures as assumed in [BSI].A.Resp-Appl, the assumption is covered by the objective.

4.4 Objectives of the sub-TSFs

4.4.1 Sub-TSF PP-0084-v2

The objectives for the sub-TSF PP-0084-v2 corresponds to the subset of the global set of objectives defined earlier in Section 4 , consisting of:

- all objectives defined in Table 9 except those specifically defined in Section Section 4.4.2 , Section Section 4.4.3 and Section Section 4.4.4 .
- the set of objectives introduced by the Authentication of the Security *IC* package and
- the set of objectives introduced by the Cryptographic Services package.

No new assets, threats, OSPs or assumptions are introduced beyond those already defined in the global SPD.

4.4.2 Sub-TSF Loader 1

The set of objectives of this sub-TSF is defined in the PP-Module “Loader 1 (for usage in secured environment only)” from [BSI-CC-PP-0125-V1]:

- [BSI.LOADER1].O.Cap_Avail_Loader1 “Capability and availability of the Loader”
- [BSI.LOADER1].OE.Lim_Block_Loader1 “Limitation of capability and blocking the Loader”

4.4.3 Sub-TSF Loader 2

The set of objectives of this sub-TSF is defined in the PP-Module “Loader 2 (for usage by authorized users only)” from [BSI-CC-PP-0125-V1]:

- [BSI.LOADER2].O.Ctrl_Auth_Loader2 “Access control and authenticity for the Loader”
- [BSI.LOADER2].OE.Usage_Loader2 “Secure communication and usage of the Loader”

The following objectives are additional ones from [Post-Deliv-Load] and additions security target operated.

- [BSI.LOADER2_ADD].O.Prot-TSF-Confidentiality “Protection of the confidentiality of the TSF”
- [BSI.LOADER2_ADD].O.Secure-UC-Code “Secure loading of the Additional Code”
- [BSI.LOADER2_ADD].O.Secure-UC-Activation “Secure activation of the Additional Code”

- [BSI.LOADER2_ADD].O.TOE-Identification “Secure identification of the TOE”
- [BSI.LOADER2_ADD].O.Secure-Load-AMemImage “Secure loading of the Additional Memory Image”
- [BSI.LOADER2_ADD].O.MemImage-Identification “Secure identification of the Memory Image”
- [BSI.LOADER2_ADD].OE.Composite-TOE-Id “Composite - TOE identification”
- [BSI.LOADER2_ADD].OE.TOE-Id “TOE identification”

4.4.4 Sub-TSF Address-based Access Control

The set of objectives of this sub-TSF is defined in the PP-Module “Address-based Access Control” from [BSI-CC-PP-0125-V1]:

- [BSI.MEMORIES].O.Addr-Access “Address-based Access Control”

5 Extended Components Definition (ASE_ECD)

5.1 Audit data storage (FAU_SAS)

This Security Target uses the extended component **FAU_SAS.1** Audit storage defined in the [BSI-CC-PP-0084-V2].

To define the security functional requirements of the *TOE* an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the *TOE* itself and because it does not give specific details of the content of the audit records.

The family “Audit data storage (FAU_SAS)” is specified as follows.

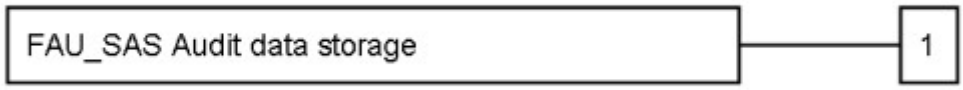
FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component levelling

Figure 4. Component leveling of Extended Component FAU_SAS



FAU_SAS.1	Requires the *TOE* to provide the possibility to store audit data.
Management	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory].

6 Security requirements (ASE_REQ)

This chapter on security requirements contains a section on security functional requirements (SFRs) for the *TOE* (Section 6.1), a section on security assurance requirements (SARs) for the *TOE* (Section 6.2), a section on the refinements of these SARs (Section 6.3) as required by the "[BSI-CC-PP-0084-V2]" Protection Profile. This chapter includes a section with the security requirements rationale (Section 6.4).

6.1 Security functional requirements for the TOE

Security Functional Requirements (SFRs) from the [BSI-CC-PP-0125-V1] Protection Profile (PP) are drawn from [CCMB-2022-11-002-R1], except the *SFR* **FAU_SAS.1**, that is extension to [CCMB-2022-11-002-R1].

This Security Target uses the extended component **FAU_SAS.1** Audit data storage defined in Section 5.1 (reproduced from the text of the [BSI-CC-PP-0084-V2] Protection Profile.)

The Security Functional Requirements of this Security Target are mainly reproduced from the [BSI-CC-PP-0084-V2]. Some iterations, assignments, selections, and refinements on SFRs have been performed according to section 8.2 of [CCMB-2022-11-002-R1]. They are easily identified in the following text and they appear ***as indicated here***. Note that in order to improve readability, iterations are sometimes expressed within tables.

In order to ease the definition and the understanding of these security functional requirements, a simplified presentation of the TOE Security Policy (*TSP*) is given in the following section.

The selected security functional requirements for the *TOE* (ST54M A01), their respective origin and type are summarized in Table 14 .

Table 14. Summary of functional security requirements for the *TOE*

Component	Component name	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	[BSI-CC-PP-0084-V2]	[CCMB-2022-11-002-R1]
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1 / Test	Limited capabilities	Abuse of functionality		
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage			External
FDP_SDC.1	Stored data confidentiality	Physical Manipulation and Probing		[CCMB-2022-11-002-R1]
FDP_SDI.2	Stored data integrity monitoring and action			
FPT_PHP.3	Resistance to physical attack			
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal *TSF* data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1 / PTG2	Random number generation (Class PTG.2)	Random Numbers		
FIA_API.1 / Auth	Authentication proof of identity	Masquerade		
FMT_LIM.1 / Loader1	Limited capabilities	Abuse of Loader Functionality		
FMT_LIM.2 / Loader1	Limited availability			
FTP_ITC.1 / Loader2	Inter-TSF trusted channel	Loader Violation		

Component	Component name	Addressing	Origin	Type
FDP_UCT.1 / Loader2	Basic data exchange confidentiality			
FDP_UIT.1 / Loader2	Data exchange integrity			
FDP_ACC.1 / Loader2	Subset access control			
FDP_ACF.1 / Loader2	Security attribute-based access control			
FCS_COP.1 / *TDES*	Cryptographic operation - *TDES*	Cipher scheme support		
FCS_COP.1 / *AES*	Cryptographic operation - *AES*			
FCS_COP.1 / Keccak-p	Cryptographic operation - Keccak-p			
FDP_ACF.1 / Memories	Security attribute-based access control	Memory Access Violation		
FDP_ACC.2 / Memories	Subset access control		This *ST*	
FMT_MSA.3 / Memories	Static attribute initialization	Correct Operation	[BSI-CC-PP-0084-V2]	
FMT_MSA.1 / Memories	Management of security attributes			
FMT_SMF.1 / Memories	Specification of management functions			
FPT_FLS.1 / Loader2	Failure with preservation of secure state	Correct Loader operation	This *ST*	
FMT_MSA.3 / Loader2	Static attribute initialization			
FMT_MSA.1 / Loader2	Management of security attribute			
FMT_SMR.1 / Loader2	Security roles			
FMT_SMF.1 / Loader2	Specification of management functions			
FIA_UID.1 / Loader2	Timing of identification			
FIA_UAU.1 / Loader2	Timing of authentication			
FAU_SAR.1 / Loader2	Audit review	Lack of *TOE* identification		
FAU_SAS.1 / Loader2	Audit storage			External
FMT_LIM.1 / Sdiag	Limited capabilities	Abuse of Secure Diagnostic functionality		[CCMB-2022-11-002-R1]
FMT_LIM.2 / Sdiag	Limited availability			
FTP_ITC.1 / Sdiag	Inter-TSF trusted channel			
FAU_SAR.1 / Sdiag	Audit review			

6.1.1 Security functional requirements regarding Malfunction

Limited fault tolerance (FRU_FLT.2)

FRU_FLT.2.1:

The *TSF* shall ensure the operation of all the *TOE*'s capabilities when the following failures occur: ***exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)***.

***Refinement**:*

The term "failure" above means "circumstances". The* TOE *prevents failures for the "circumstances" defined above.

Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1:

The *TSF* shall preserve a secure state when the following types of failures occur: ***exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.***

***Refinement**:*

The term "failure" above also covers "circumstances". The* TOE *prevents failures for the "circumstances" defined above.
Regarding application note 10 of [BSI-CC-PP-0084-V2], the secure state is reached by an immediate interrupt or by a reset, depending on the current context.
Regarding application note 11 of [BSI-CC-PP-0084-V2], the* TOE *provides information on the operating conditions monitored during Security* IC *Embedded Software execution and after a warm reset. No audit requirement is however selected in this Security Target.

6.1.2 Security functional requirements regarding Abuse of functionality

Limited capabilities (FMT_LIM.1 / Test)

FMT_LIM.1.1 / Test:

The TSF shall limit its capabilities so that in conjunction with "Limited availability (FMT_LIM.2 / Test)" the following policy is enforced: ***Limited capability and availability Policy / Test.***

SFP_1: Limited capability and availability Policy / Test
Deploying Test Features after TOE Delivery does not allow User Data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Limited availability (FMT_LIM.2 / Test)

FMT_LIM.2.1 / Test:

The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1 / Test)" the following policy is enforced: ***Limited capability and availability Policy / Test.***

SFP_1: Limited capability and availability Policy / Test
Deploying Test Features after TOE Delivery does not allow User Data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Audit storage (FAU_SAS.1)

FAU_SAS.1.1:

The TSF shall provide the test process ***before TOE Delivery*** with the capability to store ***the Initialization Data and/or Pre-personalization Data and/or supplements of the Security* IC *Embedded Software*** in the **NVM**.

6.1.3 Security functional requirements regarding Physical Manipulation and Probing

Stored data confidentiality (FDP_SDC.1)

FDP_SDC.1.1:

The TSF shall ensure the confidentiality of ***all user data*** while it is stored in ***any memory***.

Stored data integrity monitoring and action (FDP_SDI.2)

FDP_SDI.2.1:

The TSF shall monitor user data stored in containers controlled by the *TSF* for ***integrity errors*** on all objects, based on the following attributes: ***user data stored in all possible memory areas, depending on the integrity control attributes.***

FDP_SDI.2.2:

Upon detection of a data integrity error, the *TSF* shall ***signal the error and react.***

Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1:

The TSF shall resist ***physical manipulation and physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.

Refinement*:*

The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements.
Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) attacks can occur anytime and (ii) countermeasures are permanently provided.

Application note:
The TOE is physically protected by active shields that command an automatic reaction on die integrity violation detection. The TOE implements a set of countermeasures that reduce the exploitability of physical probing such as scrambling and encryption of buses and memories. So these countermeasures meet the security functional requirement of FPT_PHP.3: Resistance to physical attack.

6.1.4 Security functional requirements regarding Leakage

Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1:

The TSF shall enforce the ***Data Processing Policy*** to prevent the ***disclosure*** of user data when it is transmitted between physically-separated parts of the TOE.

Refinement:
The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically separated parts of the TOE.

Basic internal *TSF* data transfer protection (FPT_ITT.1)

FPT_ITT.1.1:

The TSF shall protect TSF data from ***disclosure*** when it is transmitted between separate parts of the TOE.

Refinement*:*

The different memories, the* CPU *and other functional units of the* TOE *(e.g. a cryptographic co-processor) are seen as separated parts of the* TOE*. This requirement is equivalent to FDP_ITT.1 above but refers to* TSF *data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1 below.

Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1:

The TSF shall enforce the ***Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security* IC *Embedded Software.***

SFP_2: Data Processing Policy User Data of the Composite TOE and TSF data shall not be accessible from the TOE *except when the Security* IC *Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security* IC *Embedded Software.*

6.1.5 Security functional requirements regarding Random Numbers

Random number generation (Class PTG.2) (FCS_RNG.1 / PTG2)

FCS_RNG.1.1 / PTG2:

The *TSF* shall provide a ***physical*** random number generator that implements the following:

- **(PTG.2.1) The *TSF* shall generate raw random numbers that can be viewed as realizations of a (time-local) stationary stochastic process R1, R2, ….**
- **(PTG.2.2) The internal random numbers shall be interpreted as realizations of random variables Y1, Y2, …. If the random variables Yj are binary-valued, it shall be Prob(Yj = 1) is in (0.493, 0.507). If the random variables Yj assume binary vectors, this condition shall be met by the projections onto the particular bits. Furthermore, it shall be guaranteed that the Shannon entropy per internal random number bit is greater than or equal to 0.9998.**
- **(PTG.2.3) The start-up test shall be applied after the *RNG* has started. It shall be designed to detect a total failure of the physical noise source and severe statistical weaknesses.The *TSF* shall not output any internal random numbers before the start-up test has been passed.**
- **(PTG.2.4) The online test shall check the quality of the raw random numbers while the *RNG* is in operation. The online test shall detect non-tolerable entropy defects of the raw random numbers sufficiently soon. The *TSF* shall not output any internal random numbers if a non-tolerable entropy defect has been detected.**
- **(PTG.2.5) The total failure test shall detect if a total failure of the physical noise source occurs while the PTRNG is in operation. The total failure test shall prevent the output of internal random numbers that depend on any raw random number that has been generated after the total failure of the physical noise source. If the PTRNG applies a cryptographic post-processing algorithm (with memory) that is compliant with functionality class DRG.2 or DRG.3, then this relaxes this requirement: After the total failure has occurred, the output of internal random numbers bits whose entropy per bit is not close to 1 shall be prevented.**

FCS_RNG.1.2 / PTG2:

The *TSF* shall provide **512-bit numbers** that meet:

- **(PTG.2.6) The internal random number shall pass test suite Tirn.**

6.1.6 Security functional requirements regarding Masquerade

Authentication proof of identity (FIA_API.1 / Auth)

FIA_API.1.1:

The TSF shall provide a ***command based on a cryptographic mechanism*** to prove the identity of ***the TOE*** by including the following properties: **CMAC *AES-256 based*** signature to an external entity.

6.1.7 Security functional requirements regarding Abuse of Loader Functionality

Limited capabilities (FMT_LIM.1 / Loader1)

FMT_LIM.1.1:

The *TSF* shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2 / Loader1)” the following policy is enforced: ***Loader Limited capability Policy.***

SFP_4: Loader Limited Capability Policy

*Deploying Loader functionality after **delivery** does not allow stored user data to be disclosed or manipulated by unauthorized user.*

Limited availability (FMT_LIM.2 / Loader1)

FMT_LIM.2.1:

The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: ***Loader Limited availability Policy***.

SFP_5: Loader Limited Availability Policy
The TSF *prevents deploying the Loader functionality after **blocking of the loader**.*

Refinement:
After blocking Loader for ST role, any execution of command does not load data to Mifare area.
After blocking Loader for ST role, any execution of command does not load data to ST area.
After blocking Loader for User role, the MemoryUpdate/Loader functionality cannot be mobilized to load data to user area.
After blocking Loader for User role, the loading capability can only be exercised through mobilizing the SDiagUserSecretErase functionality.

Note: Blocking the loader is just an option.

6.1.8 Security functional requirements regarding Loader Violation

Inter-TSF trusted channel (FTP_ITC.1 / Loader2)

FTP_ITC.1.1:

The TSF shall provide a communication channel between itself and ***ST or User*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2:

The *TSF* shall permit ***another trusted* IT *product*** to initiate communication via the trusted channel.

FTP_ITC.1.3:

The TSF shall initiate communication via the trusted channel for deploying Loader ***Maintenance transaction function***.

Refinement:
In practice, the communication is not initiated by the TSF.

Basic data exchange confidentiality (FDP_UCT.1 / Loader2)

FDP_UCT.1.1:

The *TSF* shall enforce the Loader *SFP* to receive user data in a manner protected from unauthorized disclosure.

Data exchange integrity (FDP_UIT.1 / Loader2)

FDP_UIT.1.1:

The *TSF* shall enforce the Loader *SFP* to receive user data in a manner protected from modification, deletion, insertion errors.

FDP_UIT.1.2:

The *TSF* shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

Subset access control (FDP_ACC.1 / Loader2)

FDP_ACC.1.1:

The TSF shall enforce the *Loader SFP* on:
- *the subjects* **ST *Loader, User Loader***,
- *the objects user data in* ***User*** **NVM *and*** **ST *data in*** **ST NVM**,
- *the operation deployment of Loader.*

Refinement:
The operation deployment of Loader is the Maintenance transaction.

Security attribute-based access control (FDP_ACF.1 / Loader2)

FDP_ACF.1.1:

The TSF shall enforce the ***Loader SFP*** to objects based on the following: ***all subjects, objects and attributes defined in the Loader SFP***.

FDP_ACF.1.2:

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***if the user authenticated role is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.***

Note that the term “data” also addresses Additional Code, as this code is seen as data by the TSF.

FDP_ACF.1.3:

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4:

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***none***.

The following SFP ***Loader SFP*** is defined for the requirements “Basic data exchange confidentiality (FDP_UCT.1 / Loader2)”, “Data exchange integrity (FDP_UIT.1 / Loader2)”, “Subset access control (FDP_ACC.1 / Loader2”, “Security attribute based access control (FDP_ACF.1 / Loader2)”, “Static attribute initialisation (FMT_MSA.3 / Loader2)”, and “Management of security attributes (FMT_MSA.1 / Loader2)”:

SFP_6: Loader SFP

The *TSF* must enforce that a maintenance transaction is performed if **the user authenticated is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.**
The *TSF* ruling is done according to a fixed access rights matrix, based on the subject, object and security attributes listed below.

The Security Function Policy (*SFP*) Loader *SFP* uses the following definitions:

- the subjects are the *ST* Loader and the User Loader,
  - the objects are *ST NVM* and User *NVM*,
  - the operation is Maintenance transaction,
  - the security attributes linked to the subjects are the remaining sessions, the number of consecutive authentication failures, the allowed memory areas, the logging capacity, the transaction identification. Note that subjects are authorized by cryptographic keys. These keys are considered as authentication data and not as security attributes.

6.1.9 Security functional requirements regarding Cipher scheme support

Cryptographic operation - *TDES* (FCS_COP.1 / *TDES*)

FCS_COP.1.1 / *TDES*:

The TSF shall perform ***the operations*** *in Table 15* in accordance with a specified cryptographic algorithm [**in** Table 15] and cryptographic key sizes [**of** Table 15] that meet the ***standards*** *in Table 15* .

Table 15. FCS_COP.1 - TDES

[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key size]	[assignment: list of standards]
* encryption[5] * decryption - in Cipher Block Chaining (*CBC*) mode - in Electronic Code Book (*ECB*) mode	Triple Data Encryption Standard (TDES)	112 bits, 168 bits	[sp800_67] [sp800_38a]

Cryptographic operation - *AES* (FCS_COP.1 / *AES*)

FCS_COP.1.1 / *AES*:

The TSF shall perform ***the operations*** *in Table 16* in accordance with a specified cryptographic algorithm ***in*** *Table 16* and cryptographic key sizes ***of*** *Table 16* that meet the ***standards*** *in Table 16* .

Table 16. FCS_COP.1 - AES

[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key size]	[assignment: list of standards]
* encryption (cipher) * decryption (inverse cipher) - in Cipher Block Chaining (*CBC*) mode - in Electronic Code Book (*ECB*) mode	Advanced Encryption Standard	128, 192 and 256 bits	[fips197]

Cryptographic operation - Keccak-p (FCS_COP.1 / Keccak-p)

[5] Single DES and triple DES with two keys are no longer recommended as encryption functions. Triple DES with three keys can be used until end 2027 as recommended in [eccgcm]. However depending on the context of use, the Embedded Software might need to use triple DES with two keys, in that case it is submitted to a dedicated cryptographic analysis evaluation that will take consideration of the composite product specific context of use.

FCS_COP.1.1 / Keccak-p:

The TSF shall perform ***the operations*** *in Table 17* in accordance with a specified cryptographic algorithm ***in*** *Table 17* and cryptographic key sizes ***of*** *Table 17* that meet the ***standards*** *in Table 17* .

Table 17. FCS_COP.1 - Keccak-p

[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key size]	[assignment: list of standards]
* Keccak-p[1600, n_r ={12,…, 24}], * protected Keccak-p[1600, n_r = 12, …, 24}]	Keccak-p[6]	no key for plain functions, any key length up to 256 bits for protected functions	[fips202]

6.1.10 Security functional requirements for the Memories protection

In the following, some refinements have been performed on the following SFRs:
- Security attribute-based access control (FDP_ACF.1 / Memories)
- Static attribute initialization (FMT_MSA.3 / Memories)
- Management of security attributes (FMT_MSA.1 / Memories)

These SFRs address the address-based access control of the TOE. These Address-Based Access Control SFRs and SFP have been refined in this Security Target. For the the following refinement paragraph has to be considered for each these SFR statements.

Refinement:
The SFP named "Dynamic Memory Access Control Policy SFP_3" terminology is used for the Address-based Access Control SFP of the [BSI-CC-PP-0084-V2].

The refinements of these SFRs do not change nor weaken the original requirement of the [BSI-CC-PP-0084-V2].

Security attribute-based access control (FDP_ACF.1 / Memories)

FDP_ACF.1.1:

The TSF shall enforce the ***Dynamic Memory Access Control SFP*** to objects based on the following permission control information: ***software mode, the object location, the operation to be performed, and the current set of access rights***.

FDP_ACF.1.2:

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the operation is allowed if and only if the software mode, the object location and the operation matches an entry in the current set of access rights***.

FDP_ACF.1.3:

The *TSF* shall explicitly authorize access of subjects to objects based on the following additional rules: ***None.***

FDP_ACF.1.4:

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
- in User configuration, any access (read, write, execute) to the* OST ROM *is denied,
- in User configuration, any write access to the* ST NVM *is denied.

Note: It should be noted that this level of policy detail is not needed at the application level. The composite Security Target writer should describe the *ES* access control and information flow control policies instead. Within the *ES* High

[6] [fips202] defines the Keccak-p family of permutations for any number of rounds. The standardized SHA-3 hash functions recommended in [eccgcm] and the SHAKE extendable output functions use Keccak-p[1600] with 24 rounds only. In the light of the extensive third-party cryptanalysis publicly available, there is a consensus in the community that Keccak-p[1600] with 12 rounds provides sufficient security and that this reduction in number of rounds is desirable for increasing the performance of Keccak-based functions. This state of affairs is confirmed by the definition of TurboSHAKE and KangarooTwelve, now standardized in RFC 9861. See references [fips202_sp800_185_updates], [rfc9861], [turboshake].

Level Design description, the chosen setting of *IC* security attributes would be shown to implement the described policies relying on the *IC SFP* presented here.

The SFP Dynamic Memory Access Control Policy is defined in the following:

SFP_3: Dynamic Memory Access Control Policy
The TSF *must control read, write, execute accesses of software to data, based on the software mode and on the current set of access rights.*

Subset access control (FDP_ACC.2 / Memories)

FDP_ACC.2.1:

The TSF shall enforce the ***Dynamic Memory Access Control Policy*** on ***all subjects (software), all objects (data including code stored in memories)*** and all operations among subjects and objects covered by the *SFP*.

FDP_ACC.2.2:

The TSF shall ensure that all operations between any subject controlled by the *TSF* and any object controlled by the *TSF* are covered by an access control *SFP*.

Static attribute initialization (FMT_MSA.3 / Memories)

FMT_MSA.3.1:

The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to provide ***minimally protective***[7] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2:

The TSF shall allow ***none*** to specify alternative initial values to override the default values when an object or information is created.

Application note:
The security attributes are the set of access rights currently defined. They are dynamically attached to the subjects and objects locations, i.e. each logical address.

Management of security attributes (FMT_MSA.1 / Memories)

FMT_MSA.1.1:

The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to restrict the ability to ***modify*** the security attributes: ***current set of access rights*** to ***software having the needed clearance.***

Specification of management functions (FMT_SMF.1 / Memories)

FMT_SMF.1.1:

The TSF shall be capable of performing the following management functions: ***modification of the current set of access rights security attributes by software having the needed clearance, supporting the Dynamic Memory Access Control Policy***.

6.1.11 Security functional requirements regarding Correct Loader operation

Failure with preservation of secure state (FPT_FLS.1 / Loader2)

FPT_FLS.1.1:

[7] See the ST54M_SE OS developer's guide - User Manual referenced in Table 24 for actual values

The *TSF* shall preserve a secure state when the following types of failures occur: ***the maintenance transaction is incomplete***.

Static attribute initialization (FMT_MSA.3 / Loader2)

FMT_MSA.3.1:

The *TSF* shall enforce the ***Loader SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2:

The *TSF* shall allow ***none*** to specify alternative initial values to override the default values when an object or information is created.

Management of security attribute (FMT_MSA.1 / Loader2)

FMT_MSA.1.1:

The *TSF* shall enforce the ***Loader SFP*** to restrict the ability to ***modify*** the security attributes ***remaining sessions***, ***transaction identification*** to ***the* ST *Loader or User Loader***.

Security roles (FMT_SMR.1 / Loader2)

FMT_SMR.1.1:

The *TSF* shall maintain the roles: ***ST Loader, User Loader, Secure Diagnostic, and Everybody***.

FMT_SMR.1.2:

The *TSF* shall be able to associate users with roles.

Specification of management functions (FMT_SMF.1 / Loader2)

FMT_SMF.1.1:

The *TSF* will be able to perform the following management functions: ***change the role authentication data, change the remaining sessions, block a role, under the Loader SFP***.

Timing of identification (FIA_UID.1 / Loader2)

FIA_UID.1.1:

The *TSF* shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2:

The *TSF* shall require each user to be successfully identified before allowing any other *TSF* mediated actions on behalf of that user.

Timing of authentication (FIA_UAU.1 / Loader2)

FIA_UAU.1.1:

The *TSF* shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2:

The *TSF* shall require each user to be successfully authenticated before allowing any other *TSF* mediated actions on behalf of that user.

6.1.12 Security functional requirements regarding Lack of *TOE* identification

Audit review (FAU_SAR.1 / Loader2)

FAU_SAR.1.1:

The *TSF* shall provide ***Everybody*** with the capability to read the ***Product information and the Identification of the last completed maintenance transaction, if any***, from the audit data.

FAU_SAR.1.2:

The *TSF* shall provide the audit data in a manner suitable for the user to interpret the information.

Audit storage (FAU_SAS.1 / Loader2)

FAU_SAS.1.1:

The *TSF* shall provide ***the Loader*** with the capability to store the ***transaction identification of the loaded data*** in the ***NVM***.

Refinement*:*

The TSF shall systematically store the transaction identification provided by the ST Loader or User Loader together with the loaded data.

6.1.13 Security functional requirements regarding Abuse of Secure Diagnostic functionality

Limited capabilities (FMT_LIM.1 / Sdiag)

FMT_LIM.1.1:

The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: ***Sdiag Limited Capability Policy***.

SFP_7: Sdiag Limited Capability Policy
*Deploying SDiag does not allow **User data of the Composite TOE** to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks unless the User data are submitted to an erase imposed by the User.*

Limited availability (FMT_LIM.2 / Sdiag)

FMT_LIM.2.1:

The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1 / Test)” the following policy is enforced: ***Sdiag Limited Availability Policy***.

SFP_8: Sdiag Limited Availability Policy
The SDiag capability is always deployed. Only authorized and authentic transactions can be performed. The transactions are prevented by the TSF from being performed unless the User selection of User data is effectively erased, in case the User imposes this erase. If it is not imposed by the User, the transactions can be performed without any prior User data erase.

Inter-TSF trusted channel (FTP_ITC.1 / Sdiag)

FTP_ITC.1.1:

The TSF shall provide a communication channel between itself and ***another trusted* IT *product*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2:

The TSF shall permit ***another trusted* IT *product*** to initiate communication via the trusted channel.

FTP_ITC.1.3:

The TSF shall initiate communication via the trusted channel for ***Secure Diagnostic transaction***.

***Refinement**:*
In practice, the communication is initiated by the trusted* IT *product.

Audit review (FAU_SAR.1 / Sdiag)

FAU_SAR.1.1:

The TSF shall provide ***Everybody*** with the capability to read the **NVM *User data selected area for erasure***, from the audit data.

FAU_SAR.1.2:

The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

6.2 Security assurance requirements

The ST54M A01 Security Target claims conformance to a multi-assurance evaluation level:

- A global set of SARs for the *TOE*: EAL5 augmented by ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and ASE_TSS.2.
- A specific set of SARs for each sub-TSF defined in Section 1.8 :
  - For the sub-TSF of the *PP* with additions: the SARs of the global assurance level.
  - For the sub-TSFs Loader 1, Loader 2 and Address-based Access Control: EAL6 augmented with ASE_TSS.2 and ALC_FLR.2.

Regarding application note 18 of [BSI-CC-PP-0084-V2], the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

As stated at section 6.3.3 of [BSI-CC-PP-0084-V2], the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks.

The component ALC_FLR.2 is chosen as an augmentation in this *ST* because a solid flaw management is key for the continuous improvement of the security *IC* platforms, especially on markets which need highly resistant and long lasting products.

The component ASE_TSS.2 is chosen as an augmentation in this *ST* to give architectural information on the security functionality of the TOE.

The global set of security assurance requirements (SARs) is presented in Table 18 , indicating the origin of the requirement.

The specific set of security assurance requirements (SARs) for the sub-TSFs Loader1, Loader2 and Address-based Access Control is presented in Table 19 , indicating the origin of the requirement.

Table 18. TOE global set of SARs

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5 / [BSI-CC-PP-0084-V2]
ADV_FSP.5	Complete semi-formal functional specification with additional error information	

Label	Title	Origin
ADV_IMP.1	Implementation representation of the *TSF*	
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	
AGD_OPE.1	Operational user guidance	EAL5 / [BSI-CC-PP-0084-V2]
AGD_PRE.1	Preparative procedures	
ALC_CMC.4	Production support, acceptance procedures and automation	
ALC_CMS.5	Development tools *CM* coverage	
ALC_DEL.1	Delivery procedures	
ALC_DVS.2	Sufficiency of security controls	Security Target / [BSI-CC-PP-0084-V2]
ALC_FLR.2	Flaw reporting procedures	Security Target
ALC_LCD.1	Developer defined life-cycle processes	EAL5
ALC_TAT.2	Compliance with implementation standards	
ASE_CCL.1	Conformance claims	
ASE_ECD.1	Extended components definition	
ASE_INT.1	*ST* introduction	
ASE_OBJ.2	Security objectives	
ASE_REQ.2	Derived security requirements	
ASE_SPD.1	Security problem definition	
ASE_TSS.2	*TOE* summary specification with architectural design summary	Security Target
ATE_COV.2	Analysis of coverage	EAL5 / [BSI-CC-PP-0084-V2]
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	
ATE_IND.2	Independent testing - sample	
AVA_VAN.5	Advanced methodical vulnerability analysis	Security Target / [BSI-CC-PP-0084-V2]

Table 19. TOE specific set of SARs

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL6 / [BSI-CC-PP-0084-V2]
ADV_FSP.5	Complete semi-formal functional specification with additional error information	
ADV_IMP.2	Complete mapping of the implementation representation of the *TSF*	
ADV_INT.3	Minimally complex internals	EAL6
ADV_SPM.1	Formal *TOE* security policy model	EAL6 / [BSI-CC-PP-0084-V2]
ADV_TDS.5	Complete semiformal modular design	EAL6
AGD_OPE.1	Operational user guidance	EAL6 / [BSI-CC-PP-0084-V2]
AGD_PRE.1	Preparative procedures	
ALC_CMC.5	Advanced support	
ALC_CMS.5	Development tools *CM* coverage	
ALC_DEL.1	Delivery procedures	

Label	Title	Origin
ALC_DVS.2	Sufficiency of security controls	Security Target / [BSI-CC-PP-0084-V2]
ALC_FLR.2	Flaw reporting procedures	Security Target
ALC_LCD.1	Developer defined life-cycle processes	EAL6
ALC_TAT.3	Compliance with implementation standards - all parts	
ASE_CCL.1	Conformance claims	
ASE_ECD.1	Extended components definition	
ASE_INT.1	*ST* introduction	
ASE_OBJ.2	Security objectives	
ASE_REQ.2	Derived security requirements	
ASE_SPD.1	Security problem definition	
ASE_TSS.2	*TOE* summary specification with architectural design summary	Security Target
ATE_COV.3	Rigorous analysis of coverage	EAL6 / [BSI-CC-PP-0084-V2]
ATE_DPT.3	Testing: modular design	EAL6
ATE_FUN.2	Ordered functional testing	
ATE_IND.2	Independent testing - sample	
AVA_VAN.5	Advanced methodical vulnerability analysis	Security Target / [BSI-CC-PP-0084-V2]

6.3 Refinement of the security assurance requirements

As [BSI-CC-PP-0125-V1] and [BSI-CC-PP-0084-V2] defines refinements for selected SARs, these refinements are also claimed in this Security Target.

The main customizing is that the IC Dedicated Software is an operational part of the TOE after delivery, although it is mainly not available to the user.

Regarding application note 19 of BSI-CC-PP-0084-V2, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

The text of the impacted refinements of [BSI-CC-PP-0084-V2] is reproduced in the next sections. The text of the [BSI-CC-PP-0084-V2] *SAR* refinements not impacted by this Security Target is not reproduced in the following.

An impact summary is provided in Table 20 .

Table 20. Impact of global set of SARs on [BSI-CC-PP-0084-V2] refinements

Assurance Family	BSI-CC-PP-0084-V2 Level	ST Level	Impact on refinement
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, *IC* Dedicated Software is included
ADV_IMP	1	1	None
AGD_OPE	1	1	None
AGD_PRE	1	1	New refinement related to the Loader
ALC_CMC	4	4	None
ALC_CMS	4	5	None
ALC_DEL	1	1	New refinement related to the Loader
ALC_DVS	2	2	None

Assurance Family	BSI-CC-PP-0084-V2 Level	ST Level	Impact on refinement
ATE_COV	2	2	*IC* Dedicated Software is included
AVA_VAN	5	5	None

Table 21. Impact of specific set of SARs on [BSI-CC-PP-0084-V2] refinements

Assurance Family	BSI-CC-PP-0084-V2 Level	ST Level	Impact on refinement
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, *IC* Dedicated Software is included
ADV_IMP	1	2	None
ADV_SPM	1	1	New refinement added (see below)
AGD_OPE	1	1	None
AGD_PRE	1	1	New refinement related to the Loader
ALC_CMC	4	5	None
ALC_CMS	4	5	None
ALC_DEL	1	1	New refinement related to the Loader
ALC_DVS	2	2	None
ATE_COV	2	3	*IC* Dedicated Software is included
AVA_VAN	5	5	None

6.3.1 Refinement regarding Complete semi-formal functional specification with additional error information (ADV_FSP)

~~Although the *IC*) Dedicated Test Software is a part of the *TOE*, the test functions of the *IC* Dedicated Test Software are not described in the Functional Specification because the *IC* Dedicated Test Software is considered as a test tool delivered with the *TOE* but not providing security functions for the operational phase of the *TOE*.~~ **The *IC* Dedicated Software provides security functionalities as soon as the *TOE* becomes operational (boot software). These are properly identified in the delivered documentation.**

The Functional Specification **refers to datasheet to** trace security features that do not provide any external interface but that contribute to fulfil the SFRs e.g. like physical protection. Thereby they are part of the complete instantiation of the SFRs.

The Functional Specification **refers to design specifications to detail the** mechanisms against physical attacks **described** in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those mechanisms where inspection of the layout is of relevance or tests beside the *TSFI* may be needed.

The Functional Specification **refers to data sheet to** specify operating conditions of the *TOE*. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.

All functions and mechanisms which control access to the functions provided by the *IC* Dedicated Test Software (refer to the security functional requirement (FMT_LIM.2)) **are part of the** Functional Specification. Details will be given in the document for ADV_ARC, ~~refer to Section 6.2.1.5~~. In addition, all these functions and mechanisms **are** subsequently be refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after *TOE* Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information **is** provided to allow tests and vulnerability assessment.

Since the selected higher-level assurance component requires a security functional specification presented in a “semi-formal style“ (ADV_FSP.5.2C) the changes affect the style of description, the [BSI-CC-PP-0084-V2] refinements can be applied with changes covering the *IC* Dedicated Test Software and are valid for ADV_FSP.5.

6.3.2 Refinement regarding Preparative procedures (AGD_PRE)

According to [Post-Deliv-Load]:

Preparative user guidance are intended to be used by persons responsible for the following tasks:

- acceptance of the Initial *TOE* and of the Additional Code;
- installation of the *TOE*: download of the Additional Code onto the Initial *TOE*, activation of the Additional Code, checking of the resulting Identification Data.

6.3.3 Refinement regarding Delivery procedures (ALC_DEL)

According to [Post-Deliv-Load]:

For the delivery of the Initial *TOE*, Additional Code and Final *TOE*, all the guidance describing the delivery procedures shall be taken into account.

The guidance documents for delivery procedures must especially describe the protection measures of the proof associated to the Additional Codes and the protection measures of the cryptographic keys used to generate this proof. The measures described in the guidance documents will have to be properly implemented.

6.3.4 Refinement regarding Analysis of coverage (ATE_COV)

The *TOE* **is** tested under different operating conditions within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that “Fault tolerance (FRU_FLT.2)” **is** proven for the complete *TSF*. The tests must also cover functions which may be affected by “ageing” (such as ***NVM*** writing).

The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT_PHP.3) cannot be tested in a straightforward way. Instead **STMicroelectronics provides** evidence that the *TOE* actually has the particular physical characteristics (especially layout design principles). This **is** done by checking the layout (implementation or actual) in an appropriate way. The required evidence pertains to the existence of mechanisms against physical attacks (unless being obvious).

~~The *IC* Dedicated Test Software is seen as a “test tool” being delivered as part of the *TOE*. However, the Test Features do not provide security functionality. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the *IC* Dedicated Test Software must be part of the Test Coverage Analysis~~. **The *IC* Dedicated Software provides security functionalities as soon as the *TOE* becomes operational (boot software). These are part of the Test Coverage Analysis.**

6.3.5 Refinement regarding Formal *TOE* security policy model (ADV_SPM)

This Security Target complies with the [BSI-CC-PP-0125-V1] and applies ADV_SPM.1 to the sub-TSFs defined in Section 1.8.2 , Section 1.8.3 and Section 1.8.4 .
This means that for each sub-TSF, the developer provides a formal model for the SFPs, the SFRs and proofs of the security objectives for the *TOE*.
It corresponds to SFPs given in Section 1.8 .
It corresponds to the SFRs given in Section 6.5 .

6.4 Security Requirements rationale

6.4.1 Rationale for the Security Functional Requirements

Just as for the security objectives rationale of Section 4.3 , the main line of this rationale is that the inclusion of all the security requirements of the [BSI-CC-PP-0125-V1] protection profile including the functional packages listed

in Section 1.3 , together with those introduced in this Security Target, guarantees that all the security objectives identified in Section 4 are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

Table 22. Security Requirements versus Security Objectives

Security Objective	Security Functional and Assurance Requirements
[BSI].O.Leak-Inherent	- FDP_ITT.1: Basic internal transfer protection - FPT_ITT.1: Basic internal *TSF* data transfer protection - FDP_IFC.1: Subset information flow control
[BSI].O.Phys-Probing	- FDP_SDC.1: Stored data confidentiality - FPT_PHP.3: Resistance to physical attack
[BSI].O.Malfunction	- FRU_FLT.2: Limited fault tolerance - FPT_FLS.1: Failure with preservation of secure state
[BSI].O.Phys-Manipulation	- FDP_SDI.2: Stored data integrity monitoring and action - FPT_PHP.3: Resistance to physical attack
[BSI].O.Leak-Forced	- FDP_ITT.1: Basic internal transfer protection - FPT_ITT.1: Basic internal *TSF* data transfer protection - FDP_IFC.1: Subset information flow control - FRU_FLT.2: Limited fault tolerance - FPT_FLS.1: Failure with preservation of secure state - FDP_SDI.2: Stored data integrity monitoring and action - FPT_PHP.3: Resistance to physical attack
[BSI].O.Abuse-Func	- FMT_LIM.1 / Test: Limited capabilities - FMT_LIM.2 / Test: Limited availability - FMT_LIM.1 / Sdiag: Limited capabilities - FMT_LIM.2 / Sdiag: Limited availability - FTP_ITC.1 / Sdiag: Inter-TSF trusted channel - FAU_SAR.1 / Sdiag: Audit review - FDP_ITT.1: Basic internal transfer protection - FPT_ITT.1: Basic internal *TSF* data transfer protection - FDP_IFC.1: Subset information flow control - FDP_SDC.1: Stored data confidentiality - FPT_PHP.3: Resistance to physical attack - FRU_FLT.2: Limited fault tolerance - FPT_FLS.1: Failure with preservation of secure state - FDP_SDI.2: Stored data integrity monitoring and action
[BSI].O.Identification	- FAU_SAS.1: Audit storage
[BSI].O.RND	- FCS_RNG.1 / PTG2: Random number generation (Class PTG.2) - FDP_ITT.1: Basic internal transfer protection - FPT_ITT.1: Basic internal *TSF* data transfer protection - FDP_IFC.1: Subset information flow control - FDP_SDC.1: Stored data confidentiality - FPT_PHP.3: Resistance to physical attack - FRU_FLT.2: Limited fault tolerance - FPT_FLS.1: Failure with preservation of secure state

Security Objective	Security Functional and Assurance Requirements
	- FDP_SDI.2: Stored data integrity monitoring and action
[BSI.LOADER1].O.Cap_Avail_Loader1	- FMT_LIM.1 / Loader1: Limited capabilities - FMT_LIM.2 / Loader1: Limited availability
[BSI.LOADER2].O.Ctrl_Auth_Loader2	- FTP_ITC.1 / Loader2: Inter-TSF trusted channel - FDP_UCT.1 / Loader2: Basic data exchange confidentiality - FDP_UIT.1 / Loader2: Data exchange integrity - FDP_ACC.1 / Loader2: Subset access control - FDP_ACF.1 / Loader2: Security attribute-based access control - FMT_MSA.3 / Loader2: Static attribute initialization - FMT_MSA.1 / Loader2: Management of security attribute - FMT_SMF.1 / Loader2: Specification of management functions - FMT_SMR.1 / Loader2: Security roles - FIA_UID.1 / Loader2: Timing of identification - FIA_UAU.1 / Loader2: Timing of authentication
[BSI.CRYPTO].O.Crypto-Service	- FCS_COP.1 / *TDES* / Cryptographic operation - *TDES* - FCS_COP.1 / *AES* / Cryptographic operation - *AES* - FCS_COP.1 / Keccak-p / Cryptographic operation - Keccak-p
[BSI.MEMORIES].O.Addr-Access	- FDP_ACC.2 / Memories: Subset access control - FDP_ACF.1 / Memories: Security attribute-based access control - FMT_MSA.3 / Memories: Static attribute initialization - FMT_MSA.1 / Memories: Management of security attributes - FMT_SMF.1 / Memories: Specification of management functions
[BSI.AUTH].O.Authentication	- FIA_API.1 / Auth: Authentication proof of identity
[LOADER2_ADD].O.Prot-TSF-Confidentiality	- FTP_ITC.1 / Loader2: Inter-TSF trusted channel - FDP_UCT.1 / Loader2: Basic data exchange confidentiality - FDP_UIT.1 / Loader2: Data exchange integrity - FDP_ACC.1 / Loader2: Subset access control - FDP_ACF.1 / Loader2: Security attribute-based access control - FMT_MSA.3 / Loader2: Static attribute initialization - FMT_MSA.1 / Loader2: Management of security attribute - FMT_SMF.1 / Loader2: Specification of management functions - FMT_SMR.1 / Loader2: Security roles - FIA_UID.1 / Loader2: Timing of identification - FIA_UAU.1 / Loader2: Timing of authentication - FAU_SAS.1 / Loader2: Audit storage
[LOADER2_ADD].O.Secure-UC-Code	- FTP_ITC.1 / Loader2: Inter-TSF trusted channel - FDP_UCT.1 / Loader2: Basic data exchange confidentiality - FDP_UIT.1 / Loader2: Data exchange integrity - FDP_ACC.1 / Loader2: Subset access control - FDP_ACF.1 / Loader2: Security attribute-based access control - FMT_MSA.3 / Loader2: Static attribute initialization - FMT_MSA.1 / Loader2: Management of security attribute - FMT_SMF.1 / Loader2: Specification of management functions

Security Objective	Security Functional and Assurance Requirements
	- FMT_SMR.1 / Loader2: Security roles - FIA_UID.1 / Loader2: Timing of identification - FIA_UAU.1 / Loader2: Timing of authentication - FAU_SAS.1 / Loader2: Audit storage
[LOADER2_ADD].O.Secure-UC-Activation	- FPT_FLS.1 / Loader2: Failure with preservation of secure state
[LOADER2_ADD].O.TOE-Identification	- FAU_SAS.1 / Loader2: Audit storage - FAU_SAR.1 / Loader2: Audit review - FDP_SDI.2 / Loader2_Add: Stored data integrity monitoring and action
[LOADER2_ADD].O.Secure-Load-AMemImage	- FTP_ITC.1 / Loader2: Inter-TSF trusted channel - FDP_UCT.1 / Loader2: Basic data exchange confidentiality - FDP_UIT.1 / Loader2: Data exchange integrity - FDP_ACC.1 / Loader2: Subset access control - FDP_ACF.1 / Loader2: Security attribute-based access control - FMT_MSA.3 / Loader2: Static attribute initialization - FMT_MSA.1 / Loader2: Management of security attribute - FMT_SMF.1 / Loader2: Specification of management functions - FMT_SMR.1 / Loader2: Security roles - FIA_UID.1 / Loader2: Timing of identification - FIA_UAU.1 / Loader2: Timing of authentication - FAU_SAS.1 / Loader2: Audit storage
[LOADER2_ADD].O.MemImage-Identification	- FPT_FLS.1 / Loader2: Failure with preservation of secure state - FAU_SAS.1 / Loader2: Audit storage - FAU_SAR.1 / Loader2: Audit review - FDP_SDI.2 / Loader2_Add: Stored data integrity monitoring and action
[BSI].OE.Resp-Appl	Not applicable
[BSI].OE.Process-Sec-IC	Not applicable
[BSI.LOADER1].OE.Lim_Block_Loader1	Not applicable
[BSI.LOADER2].OE.Usage_Loader2	Not applicable
[BSI.AUTH].OE.TOE_Auth	Not applicable
[SDIAG].OE.Secure-Diag-Usage	Not applicable
[LOADER2_ADD].OE.Composite-TOE-Id	Not applicable
[LOADER2_ADD].OE.TOE-Id	Not applicable

As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in Table 14 and Table 22 , it can be verified that the justifications provided by the [BSI-CC-PP-0084-V2] Protection Profile and the selected functional packages can just be carried forward to their union.

From Table 9 , it is straightforward to identify additional security objectives for the TOE: [LOADER2_ADD].O.Prot-TSF-Confidentiality, [LOADER2_ADD].O.Secure-UC-Code, [LOADER2_ADD].O.Secure-UC-Activation, [LOADER2_ADD].O.TOE-Identification, [LOADER2_ADD].O.Secure-Load-AMemImage and [LOADER2_ADD].O.MemImage-Identification introduced in this security. This rationale must show that security requirements suitably address them all. Furthermore, a careful observation of the requirements listed in Table 14 and Table 22 shows that there are security requirements introduced by this Security Target:

- FPT_FLS.1 / Loader2
- FMT_MSA.3 / Loader2
- FMT_MSA.1 / Loader2

- FMT_SMR.1 / Loader2
- FMT_SMF.1 / Loader2
- FIA_UID.1 / Loader2
- FIA_UAU.1 / Loader2
- FAU_SAR.1 / Loader2
- FAU_SAS.1 / Loader2
- FDP_ACC.2 / Memories
- FMT_LIM.1 / Sdiag
- FMT_LIM.2 / Sdiag
- FTP_ITC.1 / Sdiag
- FAU_SAR.1 / Sdiag

Though it remains to show that:

- security objectives from this Security Target, from [Post-Deliv-Load] are addressed by security requirements stated in this chapter,
- additional security requirements from this Security Target are mutually supportive with the security requirements from the [BSI-CC-PP-0125-V1] Protection Profile and selected functional packages, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in [BSI-CC-PP-0125-V1] and the selected functional packages, they form an internally consistent whole, is provided in the next subsections.

6.4.2 Additional and extended security objectives are suitably addressed

The justifications including **bold** text for modifications are reproduced from the [BSI-CC-PP-0084-V2]. Other justifications are given for the additional security objectives.

Security objective Protection against Abuse of Functionality ([BSI].O.Abuse-Func)

The justification related to the security objective Protection against Abuse of Functionality ([BSI].O.Abuse-Func) is as follows:

This objective states that abuse of functions (especially provided by the *IC* Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i.e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by “Limited availability (FMT_LIM.2) / Test” ***and*** “Limited availability (FMT_LIM.2) / Sdiag”, and the second one by “Limited capabilities (FMT_LIM.1) / Test” ***and*** “Limited capabilities (FMT_LIM.1) / Sdiag”. Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, ***these*** security functional requirements together are suitable to meet the objective.
Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective. The relevant ***Security Functional requirements*** are also listed in Table 22 .

Security objective Random Numbers ([BSI].O.RND)

The justification related to the security objective Random Numbers ([BSI].O.RND) is as follows:

“Random number generation (FCS_RNG.1 / PTG.2)” requires the *TOE* to provide random numbers of good quality. Other security functional requirements, which prevent physical manipulation and malfunction of the *TOE* (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.
Random numbers are often used by the Security *IC* Embedded Software to generate cryptographic keys for internal use. Therefore, the *TOE* shall prevent the unauthorized disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the *TOE*.

Security objective Access control and authenticity for the Loader ([BSI.LOADER2].O.Ctrl_Auth_Loader2)

The justification related to the security objective Access control and authenticity for the Loader ([BSI.LOADER2].O.Ctrl_Auth_Loader2) is as follows:

The ***security functional requirement*** "Subset access control (FDP_ACC.1) / Loader2" defines the subjects, objects and operations of the Loader *SFP* enforced by the *SFR* FTP_ITC.1 / Loader2, FDP_UCT.1 / Loader2, FDP_UIT.1 / Loader2 and FDP_ACF.1 / Loader2.

The ***security functional requirement*** "Inter-TSF trusted channel (FTP_ITC.1) / Loader2" requires the *TSF* to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.

The ***security functional requirement*** "Basic data exchange confidentiality (FDP_UCT.1) / Loader2" requires the *TSF* to receive data protected from unauthorized disclosure.

The ***security functional requirement*** "Data exchange integrity (FDP_UIT.1) / Loader2" requires the *TSF* to verify the integrity and the rightfulness of the received data.

The ***security functional requirement*** "Security attribute based access control (FDP_ACF.1) / Loader2" requires the *TSF* to implement access control for the Loader functionality.

Therefore, FTP_ITC.1 / Loader2, FDP_UCT.1 / Loader2, FDP_UIT.1 / Loader2, FDP_ACC.1 / Loader2 and FDP_ACF.1 / Loader2 with their *SFP* are suitable to meet the security objective.

Complementary, the security functional requirement "Static attribute initialization (FMT_MSA.3) / Loader2" requires that the *TOE* provides default values for security attributes.
The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "Management of security attributes (FMT_MSA.1) / Loader2" ***The security functional requirements*** "Security roles (FMT_SMR.1) / Loader2", "Timing of identification (FIA_UID.1) / Loader2" and "Timing of authentication (FIA_UAU.1) / Loader2" specify the roles that the *TSF* recognizes and the actions authorized before their identification.

The security functional requirement "Specification of management functions (FMT_SMF.1) / Loader2" provides additional controlled facility for adapting the loader behavior to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realized using the functions provided by the TOE.

Security objective Address-based Access Control ([BSI.MEMORIES].O.Addr-Access)

The justification related to the security objective Address-based Access Control ([BSI.MEMORIES].O.Addr-Access) is as follows:

The security functional requirements "Subset access control (FDP_ACC.1) / Memories" and "Security attribute based access control (FDP_ACF.1) / Memories", with the related Security Function Policy (*SFP*) ***"Memory Access Control Policy"*** exactly require to implement an area based memory access control as demanded by BSI.AAC.O.Addr-Access. Therefore, FDP_ACC.1 / Memories and FDP_ACF.1 / Memories with their *SFP* are suitable to meet the security objective.

The security functional requirement "Static attribute initialization (FMT_MSA.3) / Memories" requires that the *TOE* provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "Management of security attributes (FMT_MSA.1) / Memories". These management functions ensure that the required access control can be realized using the functions provided by the TOE.

The security functional requirement "Specification of management functions (FMT_SMF.1) / Memories" provides additional controlled facility for defining the protected sectors to the user's needs. These management functions ensure that the required access control can be realized using the functions provided by the TOE.

Security objectives Protection of the confidentiality of the TSF ([LOADER2_ADD].O.Prot-TSF-Confidentiality), Secure loading of the Additional Code ([LOADER2_ADD].O.Secure-UC-Code), and Secure loading of the Additional Memory Image ([LOADER2_ADD].O.Secure-Load-AMemImage)

The justification related to the security objectives Protection of the confidentiality of the TSF ([LOADER2_ADD].O.Prot-TSF-Confidentiality), Secure loading of the Additional Code ([LOADER2_ADD].O.Secure-UC-Code), and Secure loading of the Additional Memory Image ([LOADER2_ADD].O.Secure-Load-AMemImage) is as follows:

The security functional requirement “Subset access control (FDP_ACC.1) / Loader2” defines the subjects, objects and operations of the Loader *SFP* enforced by the SFRs FTP_ITC.1 / Loader2, FDP_UCT.1 / Loader2, FDP_UIT.1 / Loader2, FDP_ACF.1 / Loader2.

The security functional requirement “Inter-TSF trusted channel (FTP_ITC.1) / Loader2” requires the *TSF* to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.

The security functional requirement “Basic data exchange confidentiality (FDP_UCT.1) / Loader2” requires the *TSF* to receive data protected from unauthorized disclosure.

The security functional requirement “Data exchange integrity (FDP_UIT.1) / Loader2” requires the *TSF* to verify the integrity of the received data.

The security functional requirement “Security attribute based access control (FDP_ACF.1) / Loader2” requires the TSF to implement access control for the Loader functionality.

The security functional requirement “Static attribute initialization (FMT_MSA.3) / Loader2” requires that the *TOE* provides default values for security attributes.

The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement “Management of security attributes (FMT_MSA.1) / Loader2”.

The security functional requirements “Security roles (FMT_SMR.1) / Loader2”, “Timing of identification (FIA_UID.1) / Loader2” and “Timing of authentication (FIA_UAU.1) / Loader2” specify the roles that the *TSF* recognizes and the actions authorized before their identification.

The security functional requirement “Specification of management functions (FMT_SMF.1) / Loader2” provides additional controlled facility for adapting the loader behavior to the user’s needs. These management functions ensure that the required access control, associated to the loading feature, can be realized using the functions provided by the *TOE*.

The security functional requirement “Audit storage (FAU_SAS.1) / Loader2” requires to store the identification data needed to enforce that only the allowed version of the Additional Memory Image can be loaded on the Initial *TOE*.

Therefore, FTP_ITC.1 / Loader2, FDP_UCT.1 / Loader2, FDP_UIT.1 / Loader2, FDP_ACC.1 / Loader2, FDP_ACF.1 / Loader2 together with FMT_MSA.3 / Loader2, FMT_MSA.1 / Loader2, FMT_SMR.1 / Loader2, FMT_SMF.1 / Loader2, FIA_UID.1 / Loader2, FIA_UAU.1 / Loader2, and FAU_SAS.1 / Loader2 are suitable to meet these security objectives.

Security objective Secure activation of the Additional Code ([LOADER2_ADD].O.Secure-UC-Activation)

The justification related to the security objective Secure activation of the Additional Code ([LOADER2_ADD].O.Secure-UC-Activation) is as follows:

The security functional requirement “Audit storage (FAU_SAS.1) / Loader2” requires the *TSF* to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by [LOADER2_ADD].O.Secure-UC-Activation.

Therefore, FPT_FLS.1 / Loader2 is suitable to meet this security objective.

Security objective Secure identification of the TOE ([LOADER2_ADD].O.TOE-Identification)

The justification related to the security objective Secure identification of the TOE ([LOADER2_ADD].O.TOE-Identification) is as follows:

The security functional requirement “Audit storage (FAU_SAS.1) / Loader2” requires the *TSF* to store the Identification Data of the Memory Images.

The security functional requirement “Stored data integrity monitoring and action (FDP_SDI.2)” requires the *TSF* to detect the integrity errors of the stored data and react in case of detected errors.

The security functional requirement “Audit review (FAU_SAR.1) / Loader2” allows any user to read this Identification Data.

Therefore, FAU_SAS.1 / Loader2, and FAU_SAR.1 / Loader2 together with FDP_SDI.2 are suitable to meet this security objective.

Security objective Secure identification of the Memory Image ([LOADER2_ADD].O.MemImage-Identification)

The justification related to the security objective Secure identification of the Memory Image ([LOADER2_ADD].O.MemImage-Identification) is as follows:

The security functional requirement "Audit storage (FAU_SAS.1) / Loader2" requires the *TSF* to store the Identification Data of the Memory Images.

The security functional requirement "Stored data integrity monitoring and action (FDP_SDI.2)" requires the *TSF* to detect the integrity errors of the stored user data and react in case of detected errors.

The security functional requirement "Audit review (FAU_SAR.1) / Loader2" allows any user to read this Identification Data.

The security functional requirement "Audit storage (FAU_SAS.1) / Loader2" requires the *TSF* to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by [ADD].O.Secure-UC-Activation.

Therefore, FAU_SAS.1 / Loader2, FAU_SAR.1 / Loader2 together with FDP_SDI.2 and FPT_FLS.1 / Loader2 are suitable to meet this security objective.

6.4.3 Additional security requirements are consistent

These security requirements have already been argued in Section: Security objective "Access control and authenticity for the Loader ([BSI.LOADER2].O.Ctrl_Auth_Loader2)" above:

- "Static attribute initialization (FMT_MSA.3 / Loader2)"
- "Management of security attribute (FMT_MSA.1 / Loader2)"
- "Specification of management functions (FMT_SMF.1 / Loader2)"
- "Security roles (FMT_SMR.1 / Loader2)"
- "Timing of identification (FIA_UID.1 / Loader2)"
- "Timing of authentication (FIA_UAU.1 / Loader2)"

This security requirement is already argued in Section: Security objective "Address-based Access Control ([BSI.MEMORIES].O.Addr-Access)" above:

- "Subset access control (FDP_ACC.2 / Memories)"

These security requirements have already been argued in Section: Security objectives "Protection of the confidentiality of the TSF ([LOADER2_ADD].O.Prot-TSF-Confidentiality), Secure loading of the Additional Code ([LOADER2_ADD].O.Secure-UC-Code), and Secure loading of the Additional Memory Image ([LOADER2_ADD].O.Secure-Load-AMemImage)" above:

- "Static attribute initialization (FMT_MSA.3 / Loader2)"
- "Management of security attribute (FMT_MSA.1 / Loader2)"
- "Specification of management functions (FMT_SMF.1 / Loader2)"
- "Security roles (FMT_SMR.1 / Loader2)"
- "Timing of identification (FIA_UID.1 / Loader2)"
- "Timing of authentication (FIA_UAU.1 / Loader2)"
- "Audit storage (FAU_SAS.1 / Loader2)"

This security requirement is already argued in Section: Security objective "Secure activation of the Additional Code ([LOADER2_ADD].O.Secure-UC-Activation)" above:

- "Failure with preservation of secure state (FPT_FLS.1 / Loader2)"

These security requirements have already been argued in Section: Security objective "Secure identification of the *TOE* ([LOADER2_ADD].O.TOE-Identification)" above:

- "Audit storage (FAU_SAS.1 / Loader2)"
- "Audit review (FAU_SAR.1 / Loader2)"

These security requirements have already been argued in Section: Security objective "Secure identification of the Memory Image ([LOADER2_ADD].O.MemImage-Identification)" above:

- "Failure with preservation of secure state (FPT_FLS.1 / Loader2)"

- “Audit storage (FAU_SAS.1 / Loader2)”
- “Audit review (FAU_SAR.1 / Loader2)”

6.4.4 Dependencies of Security Functional Requirements

All dependencies of Security Functional Requirements have been fulfilled in this Security Target except:

- those justified in the [BSI-CC-PP-0084-V2] Protection Profile security requirements rationale,
- those justified in [BSI-CC-PP-0084-V2] selected functional packages security requirements rationale,
- the dependency of FCS_COP.1 / TDES and FCS_COP.1 / AES on FCS_CKM.6 (see discussion below),
- the dependency of FAU_SAR.1 / Loader2 on FAU_GEN.1 (see discussion below),
- the dependency of FAU_SAR.1 / Sdiag on FAU_GEN.1 (see discussion below).

Details are provided in Table 23 below.

Note that in order to avoid repetitions of the SFRs iterated in this Security Target, and improve readability, some are mentioned in a generic form in this table.

Table 23. Dependencies of security functional requirements

Label	Dependencies	In ST	From Protection Profile and functional packages
FRU_FLT.2	FPT_FLS.1	Yes	Yes, from [BSI-CC-PP-0084-V2]
FPT_FLS.1	None	No dependency	N/A
FMT_LIM.1 / Test	FMT_LIM.2 / Test	Yes	Yes, from [BSI-CC-PP-0084-V2]
FMT_LIM.2 / Test	FMT_LIM.1 / Test	Yes	Yes, from [BSI-CC-PP-0084-V2]
FDP_SDC.1	None	No dependency	N/A
FDP_SDI.2	None	No dependency	N/A
FPT_PHP.3	None	No dependency	N/A
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1.	Yes, by: - FDP_IFC.1	Yes, FDP_IFC.1 is from [BSI-CC-PP-0084-V2]
FPT_ITT.1	None	No dependency	N/A
FDP_IFC.1	FDP_IFF.1	No, see [BSI-CC-PP-0084-V2]	Yes, see [BSI-CC-PP-0084-V2]
FCS_RNG.1 / PTG2	None	No dependency	N/A
FIA_API.1 / Auth	None	No dependency	N/A
FMT_LIM.1 / Loader1	FMT_LIM.2 / Loader1	Yes	Yes, from [BSI-CC-PP-0084-V2]
FMT_LIM.2 / Loader1	FMT_LIM.1 / Loader2	Yes	Yes, from [BSI-CC-PP-0084-V2]
FTP_ITC.1 / Loader2	None	No dependency	N/A
FDP_UCT.1 / Loader2	FTP_ITC.1 / Loader2 or FTP_TRP.1 / Loader2 or FDP_ACC.1 / Loader2 or FDP_IFC.1 / Loader2.	Yes, by: - FTP_ITC.1 / Loader2 - FDP_ACC.1 / Loader2	Yes, FTP_ITC.1 / Loader2 is from [BSI-CC-PP-0084-V2] Yes, FDP_ACC.1 / Loader2 is from [BSI-CC-PP-0084-V2]
FDP_UIT.1 / Loader2	FDP_ACC.1 / Loader2 or FDP_IFC.1 / Loader2 or FTP_ITC.1 / Loader2 or FTP_TRP.1 / Loader2.	Yes, by: - FDP_ACC.1 / Loader2 - FTP_ITC.1 / Loader2	Yes, FDP_ACC.1 / Loader2 is from [BSI-CC-PP-0084-V2] Yes, FTP_ITC.1 / Loader2 is from [BSI-CC-PP-0084-V2]
FDP_ACC.1 / Loader2	FDP_ACF.1 / Loader2	Yes	Yes, from [BSI-CC-PP-0084-V2]
FDP_ACF.1 / Loader2	FDP_ACC.1 / Loader2	Yes	Yes, from [BSI-CC-PP-0084-V2]

Label	Dependencies	In ST	From Protection Profile and functional packages
	FMT_MSA.3 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
FCS_COP.1 / *TDES*	FCS_CKM.6	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
FCS_COP.1 / *AES*	FCS_CKM.6	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
FCS_COP.1 / Keccak-p	FCS_CKM.6	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5	No, see discussion below	Yes, from [BSI-CC-PP-0084-V2]
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes	No, from [CCMB-2022-11-002-R1]
	FMT_MSA.3 / Memories	Yes	Yes, from [BSI-CC-PP-0084-V2]
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, from [BSI-CC-PP-0084-V2]
	FMT_SMR.1 / Memories	No, see [BSI-CC-PP-0084-V2]	Yes, from [BSI-CC-PP-0084-V2]
FMT_MSA.1 / Memories	FMT_SMR.1 / Memories	No, see [BSI-CC-PP-0084-V2]	Yes, from [BSI-CC-PP-0084-V2]
	FMT_SMF.1 / Memories	Yes	Yes, from [BSI-CC-PP-0084-V2]
	FDP_ACC.1 / Memories or FDP_IFC.1 / Memories.	Yes by FDP_ACC.2 / Memories	Yes, from [BSI-CC-PP-0084-V2]
FMT_SMF.1 / Memories	None	No dependency	N/A
FPT_FLS.1 / Loader2	None	No dependency	N/A
FMT_MSA.3 / Loader2	FMT_MSA.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
	FMT_SMR.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
FMT_MSA.1 / Loader2	FMT_SMR.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
	FMT_SMF.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
	FDP_ACC.1 / Loader2 or FDP_IFC.1 / Loader2.	Yes, by: - FDP_ACC.1 / Loader2	Yes, from [BSI-CC-PP-0084-V2]
FMT_SMR.1 / Loader2	FIA_UID.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]
FMT_SMF.1 / Loader2	None	No dependency	N/A
FIA_UID.1 / Loader2	None	No dependency	N/A
FIA_UAU.1 / Loader2	FIA_UID.1 / Loader2	Yes	No, from [CCMB-2022-11-002-R1]

Label	Dependencies	In ST	From Protection Profile and functional packages
FAU_SAR.1 / Loader2	FAU_GEN.1 / Loader2	No, by FAU_SAS.1 / Loader2 instead, see discussion below	No, from [CCMB-2022-11-002-R1]
FMT_LIM.1 / Sdiag	FMT_LIM.2 / Sdiag	Yes	No, from [CCMB-2022-11-002-R1]
FMT_LIM.2 / Sdiag	FMT_LIM.1 / Sdiag	Yes	No, from [CCMB-2022-11-002-R1]
FTP_ITC.1 / Sdiag	None	No dependency	N/A
FAU_SAR.1 / Sdiag	FAU_GEN.1 / Sdiag	No, see discussion below	No, from [CCMB-2022-11-002-R1]
FDP_ACC.2 / Memories	FDP_ACF.1 / Memories	Yes	Yes, from [BSI-CC-PP-0084-V2]
FAU_SAS.1	None	No dependency	N/A
FAU_SAS.1 / Loader2	None	No dependency	N/A

Part 2 of the Common Criteria defines the dependency of “Cryptographic operation (FCS_COP.1)” on “Import of user data without security attributes (FDP_ITC.1)” or “Import of user data with security attributes (FDP_ITC.2)” or “Cryptographic key generation (FCS_CKM.1)”. In this particular *TOE*, the *ES* has all possibilities to implement its own creation function, in conformance with its security policy.

Part 2 of the Common Criteria defines the dependency of “Cryptographic operation (FCS_COP.1)” on “Timing and event of cryptographic key destruction (FCS_CKM.6)”. In this particular *TOE*, there is no specific function for the destruction of the keys. The *ES* has all possibilities to implement its own destruction function, in conformance with its security policy. Therefore, FCS_CKM.6 is not defined in this *ST*.

Part 2 of the Common Criteria defines the dependency of “Audit review (FAU_SAR.1) / Loader2” on “Audit data generation (FAU_GEN.1)”. In this particular *TOE*, “Audit storage (FAU_SAS.1) / Loader2” is used to ensure the storage of audit data, because FAU_GEN.1 is too comprehensive to be used in this context. Therefore this dependency is fulfilled by “Audit storage (FAU_SAS.1) / Loader2” instead.

Part 2 of the Common Criteria defines the dependency of “Audit review (FAU_SAR.1) / Sdiag” on “Audit data generation (FAU_GEN.1)”. In this particular *TOE*, there is no specific function for audit data generation, the data to be audited are just stored. Therefore, FAU_GEN.1 is not defined in this *ST*.

6.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach the EALs selected in this Security Target for the *TOE* multi-assurance evaluation level

The ST54M A01 Security Target claims conformance to a multi-assurance evaluation level:

- A global set of SARs for the *TOE*: EAL5 augmented by ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 and ASE_TSS.2.
- A specific set of SARs for each sub-TSF defined in Section 1.8 :
  - For the sub-TSF of the *PP* with additions: the SARs of the global assurance level.
  - For the sub-TSFs Loader 1, Loader 2 and Address-based Access Control: EAL6 augmented with ASE_TSS.2 and ALC_FLR.2.

Regarding application note 18 of [BSI-CC-PP-0084-V2], this multi-assurance Security Target chooses this multi-assurance level with augmentations because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

For the TOE global set of SARs *EAL*5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, and improved mechanisms and/or procedures that provide confidence that the *TOE* will not be tampered during development.

For the specific set of *SARs EAL*6 represents a meaningful increase in assurance from EAL4 by requiring a formal security policy model, semiformal design descriptions, a more structured (and hence analyzable) architecture,

extensive testing, and improved mechanisms and/or procedures that provide confidence that the *TOE* will not be tampered during development.

The component ALC_FLR.2 is chosen as an augmentation in this *ST* because a solid flaw management is key for the continuous improvement of the security *IC* platforms, especially on markets which need highly resistant and long lasting products.

The component ASE_TSS.2 is chosen as an augmentation in this *ST* to give architectural information on the security functionality of the *TOE*.

The assurance components in an evaluation assurance level (*EAL*) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5 and EAL6. Therefore, these components add additional assurance to EAL5 for the global set of SARs and EAL6 for the specific set of SARs, but the mutual support of the requirements and the internal consistency is still guaranteed.

Note that detailed and updated refinements for assurance requirements are given in Section 6.3 .

Dependencies of global set of assurance requirements

Dependencies of global set of security assurance requirements are fulfilled by the EAL5 package selection.

The augmentation to this package identified in Section 6.2 does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_DVS.2 and AVA_VAN.5 dependencies have been justified in [BSI-CC-PP-0084-V2]
- ALC_FLR.2 has no dependency.
- ASE_TSS.2 dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this *ST*.

Dependencies of specific set of assurance requirements

Dependencies of the specific set of security assurance requirements are fulfilled by the EAL6 package selection.

The augmentation to this package identified in Section 6.2 does not introduce dependencies not already satisfied by the EAL6 package, and is considered as consistent augmentation:

- ALC_FLR.2 has no dependency.
- ASE_TSS.2 dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this *ST*.

6.5 Security Functional Requirements of the sub-TSFs

6.5.1 Sub-TSF PP-0084-v2

The SFRs implemented by the sub-TSF PP-0084-v2 are derived from the global set of SFRs defined in Table 14 . The sub-TSF PP-0084-v2 is responsible for all SFRs listed in Table 14 , except those specifically allocated to the sub-TSFs defined in Section 6.5.2 , Section 6.5.3 , and Section 6.5.4 .

6.5.2 Sub-TSF Loader 1

The SFRs of this sub-TSF, defined in the PP-Module “Loader 1 (for usage in secured environment only)” from [BSI-CC-PP-0125-V1], consist of:

- FMT_LIM.1 / Loader1
- FMT_LIM.2 / Loader1

6.5.3 Sub-TSF Loader 2

The SFRs of this sub-TSF, defined in the PP-Module “Loader 2 (for usage by authorized users only)” from [BSI-CC-PP-0125-V1], consist of:

- FTP_ITC.1 / Loader2
- FDP_UCT.1 / Loader2
- FDP_UIT.1 / Loader2
- FDP_ACC.1 / Loader2
- FDP_ACF.1 / Loader2
- FPT_FLS.1 / Loader2
- FMT_MSA.3 / Loader2
- FMT_MSA.1 / Loader2
- FMT_SMR.1 / Loader2
- FMT_SMF.1 / Loader2
- FIA_UID.1 / Loader2
- FIA_UAU.1 / Loader2
- FAU_SAR.1 / Loader2
- FAU_SAS.1 / Loader2

6.5.4 Sub-TSF Address-based Access Control

The SFRs of this sub-TSF, defined in the PP-Module “Address-based Access Control” from [BSI-CC-PP-0125-V1], consist of:

- FDP_ACC.2 / Memories
- FDP_ACF.1 / Memories
- FMT_MSA.3 / Memories
- FMT_MSA.1 / Memories
- FMT_SMF.1 / Memories

7 TOE summary specification (ASE_TSS)

This section demonstrates how the *TOE* meets each Security Functional Requirement, which will be further detailed in the ADV_FSP documents.

7.1 TOE Security Functional Requirements realization

This section argues how the *TOE* meets each *SFR*.

7.1.1 Limited fault tolerance (FRU_FLT.2)

The *TSF* provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to random number generation, power supply, data flows and cryptographic operations, thus preventing risk of malfunction.

7.1.2 Failure with preservation of secure state (FPT_FLS.1)

The *TSF* provides preservation of secure state by detecting and managing the following events, resulting in an immediate interruption or reset:

- Die integrity violation detection,
- Errors on memories and registers,
- Glitches on external power supply lines,
- High voltage supply,
- *CPU* errors,
- *MPU* errors,
- Detection of out of bound access on memories and registers,
- Faults on crypto processors.

The *ES* can generate a software reset.

7.1.3 Limited capabilities (FMT_LIM.1 / Test), Limited availability (FMT_LIM.2 / Test), Limited capabilities (FMT_LIM.1 / Loader1), Limited availability (FMT_LIM.2 / Loader1), Limited capabilities (FMT_LIM.1 / Sdiag) and Limited availability (FMT_LIM.2 / Sdiag)

The *TOE* is either in Test, Admin or User configuration.

The *TOE* may also be in Basic Diagnostic (aka Diagnostic) or Secure Diagnostic volatile configuration.

The Test and Diagnostics configurations are reserved to *ST*.

The *TSF* ensures the switching and the control of *TOE* configuration, the corresponding access control and the control of the corresponding capabilities. The transition controls rely on several strong mechanisms .

The *TSF* reduces the available features depending on the *TOE* configuration.

7.1.4 Stored data confidentiality (FDP_SDC.1)

The *TSF* ensures confidentiality of the User Data, thanks to the following features:

- Memories scrambling and encryption,
- Protection of *NVM* sectors,
- *MPU*,
- *LPU* and
- Active shields.

7.1.5 Stored data integrity monitoring and action (FDP_SDI.2)

The *TSF* ensures integrity of the stored data, thanks to the following features:

- Memories *EDC* (Error Detecting Code) / *ECC* (Error Correcting Code),
- *MPU*,
- *LPU*.

7.1.6 Resistance to physical attack (FPT_PHP.3)

The *TSF* ensures resistance to physical tampering, thanks to the following features:

- The *TOE* implements a set of countermeasures that reduce the exploitability of physical probing.
- The *TOE* is physically protected by active shields that command an automatic reaction on die integrity violation detection.

7.1.7 Basic internal transfer protection (FDP_ITT.1), Basic internal *TSF* data transfer protection (FPT_ITT.1) and Subset information flow control (FDP_IFC.1)

The *TSF* prevents the disclosure of internal and user data thanks to:

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment.

7.1.8 Random number generation (Class PTG.2) (FCS_RNG.1 / PTG2)

The *TSF* provides true random numbers that can be qualified with the test metrics required by the [bsi_ais_31] standard for a PTG.2 class device.

7.1.9 Authentication proof of identity (FIA_API.1 / Auth)

In Admin configuration, the System Firmware provides commands based on a cryptographic mechanism which allows another *IT* product to check that the *TOE* is a genuine *TOE*.

7.1.10 Inter-TSF trusted channel (FTP_ITC.1 / Loader2), Basic data exchange confidentiality (FDP_UCT.1 / Loader2), Data exchange integrity (FDP_UIT.1 / Loader2) and Audit storage (FAU_SAS.1 / Loader2)

In Admin configuration, the System Firmware provides a secure channel to allow another *IT* product to operate a maintenance transaction.

The ciphered data is automatically decrypted then stored in the requested memory.

A maintenance transaction can end only after a successful integrity check of the loaded data or an erase. The identification data associated with the memory update is automatically logged during the session.

7.1.11 Subset access control (FDP_ACC.1 / Loader2) and Security attribute-based access control (FDP_ACF.1 / Loader2)

In Admin configuration, during a maintenance transaction, the System Firmware verifies if the Loader access conditions are satisfied and returns an error when this is not the case.

In particular, the additional memory update must be intended to be assembled with the memory update previously loaded.

7.1.12 Cryptographic operation - *TDES* (FCS_COP.1 / *TDES*)

The *TOE* provides optionally an *EDES+* accelerator that has the capability to perform Triple *DES* encryption and decryption in Electronic Code Book (*ECB*) and Cipher Block Chaining (*CBC*) modes conformant to *NIST* SP 800-67 and *NIST* SP 800-38A.

7.1.13 Cryptographic operation - *AES* (FCS_COP.1 / *AES*)

The *TOE* provides optionally an *AES* accelerator allowing the following standard *AES* cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to *FIPS PUB* 197 for operations:

- cipher,
- inverse cipher.
- Electronic Code Book (*ECB*) and Cipher Block Chaining (*CBC*) modes.

These operations include intrinsic counter-measures against attacks.

7.1.14 Cryptographic operation - Keccak-p (FCS_COP.1 / Keccak-p)

The Keccak-p accelerator provides a toolbox for building modes on top of the following permutations, conformant to *FIPS* 202:

- Keccak-p[1600, n_r from 12 to 24].

The Keccak-p accelerator provides a toolbox for building modes on top of the following permutations, conformant to *FIPS* 202, offering resistance against side channel and fault attacks:

- protected Keccak-p[1600, n_r from 12 to 24].

7.1.15 Security attribute-based access control (FDP_ACF.1 / Memories) and Subset access control (FDP_ACC.2 / Memories)

The *TOE* enforces the dynamic memory management policy for data access and code access thanks to a dynamic Memory Protection Unit (*MPU*) and a Library Protection Unit (*LPU*), programmed by the *ES*.

Overriding the *MPU* and *LPU* set of access rights, depending on the *TOE* configuration, the *TOE* enforces additional protections on specific parts of the memories.

7.1.16 Static attribute initialization (FMT_MSA.3 / Memories)

The *TOE* enforces a default memory management policy when none other is programmed by the *ES*.

7.1.17 Management of security attributes (FMT_MSA.1 / Memories) and Specification of management functions (FMT_SMF.1 / Memories)

The *TOE* provides a dynamic Memory Protection Unit (*MPU*) offering protection with dedicated access permission to 16 different memory regions, that can be configured by the *ES*.

The Library Protection Unit (*LPU*) offers complementary memory protections, that can be configured in Admin configuration, in case the *LPU* is not reserved to *ST*.

7.1.18 Failure with preservation of secure state (FPT_FLS.1 / Loader2)

In Admin configuration, the System Firmware provides preservation of secure state by forcing a reset if an abnormal behavior is detected.

It also enforces that a maintenance transaction can only end when it is consistent or canceled by an erase.

7.1.19 Static attribute initialization (FMT_MSA.3 / Loader2)

In Admin configuration, the System Firmware provides restrictive default values for the Flash Loader security attributes.

7.1.20 Management of security attribute (FMT_MSA.1 / Loader2) and Specification of management functions (FMT_SMF.1 / Loader2)

In Admin configuration, the System Firmware provides the capability for an authorized user to change part of the Flash Loader security attributes.

7.1.21 Security roles (FMT_SMR.1 / Loader2)

The System Firmware supports the assignment of roles to users through the assignment of different keys for the different roles. This allows to distinguish between the roles of *ST* Loader, User Loader, Secure Diagnostic, and Everybody.

7.1.22 Timing of identification (FIA_UID.1 / Loader2) and Timing of authentication (FIA_UAU.1 / Loader2)

The System Firmware identifies the user through the key selected for authentication. This is performed by verifying an encryption, thus preventing to unveil the key.

After this authentication, both parties share a session key.

A limited number of operations is allowed on behalf of the user before the user is identified and authenticated, such as boot, authentication and non-critical queries.

7.1.23 Audit review (FAU_SAR.1 / Loader2)

In Admin configuration, the System Firmware allows to read the product information and the identification data of all memory updates previously loaded on the *TOE*.

7.1.24 Inter-TSF trusted channel (FTP_ITC.1 / Sdiag)

In Secure Diagnostic volatile configuration, the System Firmware provides a secure channel to allow another *IT* product to operate a Secure Diagnostic transaction.

7.1.25 Audit review (FAU_SAR.1 / Sdiag)

The System Firmware allows to read the User data selected area for erasure.

7.1.26 Audit storage (FAU_SAS.1)

In User configuration, the *TOE* provides commands to store data and/or pre-personalization data and/or supplements of the *ES* in the *NVM*. These commands are only available to authorized processes before delivery.

8 *TOE* guidance and sites lists

Table 24. Guidance documents

Component description	Reference	Version
NFC controller and secure element system in package - ST54M preliminary datasheet	DS_ST54M	0.3
ST54M_SE OS developer's guide - Preliminary data - User Manual	UM_ST54M_SE	0.6
ST54M_SE firmware - User manual	UM_ST54M_SE_FW	7
Arm® Cortex-M35P Processor Technical Reference Manual	100883_0102_00_en	r1p2
Security guidance of the ST54M_SE secure MCU subsystem - Application note	AN_SECU_ST54M_SE	1
Random number generation V1.4 for ST54M_SE - User manual	UM_ST54M_SE_TRNG14	1

Table 25. Sites list

Site	Address	Activities[8]
AMTC / Toppan Dresden	Advanced Mask Technology Center Gmbh & Co KG Rahnitzer Allee 9 01109 Dresden Germany	MASK
ARDENTEC Taiwan T	Ardentec Corporation No.3, Gongye 3rd Rd., Hsin-Chu Industrial Park, Hukou Township, Hsinchu County 303036, Taiwan, R.O.C.	EWS
DNP	Dai Nippon printing Co ltd. 2-2-1 KAMI-FUKUOKA, Fujimino-shi, Saitama,356-8507 Japan	MASK
DPE	Dai Printing Europe Via C. Olivetti, 2/A, I-20041 Agrate, Italy	MASK
Feiliks	Feili Logistics (Shenzhen) CO., Ltd. Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHS WHSD
JCAP	JCET Advanced Packaging Co.,Ltd No.78 Changshan Rd,Jiangyin,Jiangsu, China	BE
Pantos	LX Pantos Logistics (HK) Co Ltd. Unit 1001, 10/F, Mapletree Logistics Hub, 30 Tsing Yi Road, Tsing Yi, N.T., Hong Kong	WHSD
ST AMK1	STMicroelectronics 5A Serangoon North Avenue 5 Singapore 554574	DEV

[8]DEV = development, FE = front end manufacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask preparation or mask manufacturing, WHS = internal warehouse, WHSD = warehouse for delivery, IT = Information Technology.

Site	Address	Activities[9]
ST AMK6	STMicroelectronics 18 Ang Mo Kio Industrial park 2 Singapore 569505	WHS WHSD
ST Catania	STMicroelectronics Str. Primosole, 50, 95121 Catania, Italy	DEV
ST Crolles	STMicroelectronics 850 rue Jean Monnet 38926 Crolles France	DEV FE MASK
ST Gardanne	CMP Georges Charpak 880 Avenue de Mimet 13541 Gardanne France	BE
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	BE DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive Singapore 508938	WHSD
ST Palermo	STMicroelectronics Via Tommaso Marcellini, 8L, 90129 Palermo, Italy	DEV
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark 35700 Rennes France	DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, 13106 Rousset Cedex France	DEV EWS WHSD
ST Sophia	STMicroelectronics 635 route des lucioles 06560 Valbonne France	DEV
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh Singapore 19521	EWS
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana Tunisia	IT
Suzhou	STMicroelectronics C8-2/C9-2 warehouse, 8 Datong Road,	WHSD

[9]DEV = development, FE = front end manufacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask preparation or mask manufacturing, WHS = internal warehouse, WHSD = warehouse for delivery, IT = Information Technology.

Site	Address	Activities[10]
	Integrated Free Trade Zone, New District, Suzhou, 215151, P.R. China	
STS Shenzhen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone Shenzhen P.R. China 518038	BE EWS
STS Shenzhen Lab	STS Microelectronics 17 Taohua Road, Futian free trade zone, Shenzhen P.R. China 518038	BE
WINSTEK	Winstek Semiconductor Co., Ltd. No 176-5, Luliaokeng, 6th Ling, Qionglin, 307 Hsinchu County, Taiwan	BE

[10]DEV = development, FE = front end manufacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask preparation or mask manufacturing, WHS = internal warehouse, WHSD = warehouse for delivery, IT = Information Technology.

9 Reference documents

Table 26. Common Criteria

Reference	Description
[BSI-CC-PP-0084-V2]	Security IC Platform Protection Profile including Functional Packages., Eurosmart.
[BSI-CC-PP-0125-V1]	Security IC Platform Multi-assurance PP-Configurations., Eurosmart.
[CCMB-001-ERA]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) - Version 1.2., CCMB.
[CCMB-2022-11-001-R1]	Common Criteria for Information Technology Security Evaluation - Part 1 Introduction and general model, CCMB.
[CCMB-2022-11-002-R1]	Common Criteria for Information Technology Security Evaluation - Part 2 Security functional components, CCMB.
[CCMB-2022-11-003-R1]	Common Criteria for Information Technology Security Evaluation - Part 3 Security assurance components, CCMB.
[CCMB-2022-11-005-R1]	Common Criteria for Information Technology Security Evaluation - Part 5 Pre-defined packages of security requirements, CCMB.
[Post-Deliv-Load]	Security requirements for post-delivery code loading. Version 2.0, JIL.

Table 27. Other standards documents

Reference	Description
[bsi_ais_31]	Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS 31, Version 4., URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Anwendungshinweise-und-Interpretationen/anwendungshinweise-und-interpretationen_node.html.
[eccgcm]	European Cybersecurity Certification Group Sub-group on Cryptography, version 2.0, ECCG Sub-group on Cryptography, URL: https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf&prefLang=da.
[fips197]	FIPS PUB 197 - Advanced Encryption Standard (AES), Morris Dworkin and Elaine Barker and James Nechvatal and James Foti and Lawrence Bassham and E. Roback and James Dray.
[fips202]	FIPS PUB 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Morris Dworkin.
[fips202_sp800_185_updates]	Public Comments on the Decision Proposal to Update FIPS 202 and Revise NIST SP 800-185, NIST.
[fips203]	FIPS PUB 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard, NIST.
[fips204]	FIPS PUB 203 - Module-Lattice-Based Digital Signature Standard, NIST.
[ieee1363]	IEEE Std 1363-2000: IEEE Standard Specifications for Public-Key Cryptography, The Institute of Electrical and Electronics Engineers, Inc., URL: https://books.google.nl/books?id=KKc8nQAACAAJ.
[ieee1363a]	IEEE 1363a-2004: IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques, The Institute of Electrical and Electronics Engineers, Inc., URL: https://books.google.nl/books?id=KKc8nQAACAAJ.
[iso14888]	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO, ISO/IEC.
[iso9796]	ISO/IEC 9796-2, Information technology - Security Techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms, ISO/IEC.
[pkcs1v21]	PKCS #1 v2.1 RSA Cryptography Standard, RSA Laboratories.

Reference	Description
[rfc9861]	KangarooTwelve and TurboSHAKE, B. Viguier, D. Wong, G. Van Assche, Q. Dang, J. Daemen.
[sp800_38a]	SP 800-38A - Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris Dworkin.
[sp800_67]	NIST SP 800-67 Rev. 2 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Elaine Barker and Nicky Mouha.
[turboshake]	TurboSHAKE, Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, Ronny Van Keer and Benoît Viguier.

10 Glossary

Table 28. **Glossary**

Term	Definition
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Loader	The Loader is the software developed by the Product Manufacturer. It is used to load and activate the Additional Code into the Product FLASH memory. The Loader is included in the dedicated software and is part of the Initial TOE.
Security IC	Composition of the TOE, the Security IC Embedded Software, User Data, and the package.
Arm®	Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
Composite product	Security IC product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by ST. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
Security IC Embedded Software (ES)	Software embedded in the Security IC and not developed by the IC designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3.
TOE Delivery	The period when the TOE is delivered which is after Phase 3 or Phase 1 for the NesLib, in this Security Target.
Sensitive information	Any information identified as a security relevant element of the TOE such as: • the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data), • the security IC embedded software, • the IC dedicated software, • the IC specification, design, development tools and technology.
User data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.
Security services	Immutable secure services are mainly composed of Debug Authentication, STiRoT, and the secure library.
Secret	Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
Pre-personalization data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases. If “Package 2':‘ Loader dedicated for usage by authorized users only“ is used the Pre-personalisation Data may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.
IC Dedicated Test Software	That part of the IC Dedicated Software which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Test features	All features and functions (implemented by the IC Dedicated Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.
IC manufacturer	Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Authorized User	A user who may, in accordance with the TSP, perform an operation.
Initial TOE	From the loader perspective, the Initial TOE is the product on which the Additional Code is loaded and with the Loader as part of the embedded software. Here the term TOE denotes the TOE itself as well as the composite TOE which both may be maintained by loading of an additional memory image.

Term	Definition
Final TOE	From the loader perspective, the Final TOE is generated from the Initial TOE and the Additional Code. It is the resulting product of the Atomic Activation of the Additional Code onto the Initial TOE. Here the term TOE denotes the TOE itself as well as the composite TOE considered as a memory image which both may be maintained by a maintenance transaction.
End-consumer	User of the Composite Product in Phase 7.
Additional Code	From the loader perspective, code activated by the Atomic Activation on the Initial TOE to generate the final TOE. For instance, Additional Code could: correct flaws, add new functionalities, update the operating system. An Additional Code is a particular « memory image » that has been activated in an authorized way on behalf of the TOE owner.
Memory image	Set of mappings of memory addresses onto data.
Atomic activation	The Loader guarantees at activation time that the loaded Additional Code is activated and that the Identification Data of the TOE are updated. This functionality is called Atomic Activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.
Subject	An entity within the TSC that causes operations to be performed.
Security attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

11 Abbreviations

Table 29. **Abbreviations**

Term	Definition
AES	Advanced Encryption Standard
BE	Back End manufacturing
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining
CC	Common Criteria
CM	Counter Measures
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DESFire	MIFARE® DESFire® EV1
DEV	Hardware and software development
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
EDC	Error Detection Code
EDES	Enhanced DES
ES	Security IC Embedded Software
ES_DEV	Libraries development
EWS	Electrical Wafer Sort
FE	Front End manufacturing
FIPS	Federal Information Processing Standard
GPIO	General Purpose I/O
I/O	Input / Output
IART	ISO-7816 Asynchronous Receiver Transmitter
IC	Integrated Circuit
ISO	International Standards Organisation
IT	Information Technology
LPU	Library Protection Unit
MASK	Mask preparation or Mask manufacturing
MPU	Microprocessor Unit
NESCRYPT	Next Step Cryptography Accelerator
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NVM	Non Volatile Memory
OS	Operating System
OST	Operating System for Test
PP	Protection Profile

Term	Definition
PUB	Publication Series
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
ST	Context dependent: STMicroelectronics or Security Target
SWP	Single-Wire Protocol
TDES	Triple Data Encrypption Standard
TOE	Target Of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	TOE Security Policy
WHS	Internal Warehouse
WHSD	Warehouse for Delivery

IMPORTANT NOTICE - READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.